NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

TESTING AND EVALUATION OF SHIPBOARD WIRELESS NETWORK COMPONENTS

by

Richard J. McConnell

March 2000

Thesis Advisor: Xiaoping Yun
Second Reader: Herschel H. Loomis

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE March 2000

3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE Testing and Evaluation of Shipboard Wireless Network Components

5. FUNDING NUMBERS

6. AUTHOR(S) Richard J. McConnell

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

Fundamental challenges facing program managers and information technology decision makers today are the identification of architectures and technologies that reduce the cost of maintaining computer networks while simultaneously increasing worker productivity. Advances in wireless communications and subsequently, wireless local area networks (WLANs) permit mobile users to share information without being hardwired to a network. These mobile devices will enable shipboard personnel to submit damage control reports, update equipment logs, view technical manuals and order repair parts, without being confined by the limitations of a wired network. The advantages of WLANs are virtually endless, ranging from the uses previously discussed, to communications between the ship and its small boats, to automated data transfer of degaussing results, and even direct parts ordering from a pier-side supply center.

This thesis provides a hardware analysis and discusses coverage limitations of commercially available WLAN components for use onboard naval vessels. Utilization of this mobile equipment will improve DC communications and watchstander productivity. With remote access to the wired network backbone, personnel can conduct transactions instantaneously whenever and wherever the need arises. A discussion of the theories and principles governing the operation of WLANs is presented, followed by a laboratory evaluation of current, commercially available components.

14. SUBJECT TERMS Wireless Local Area Networks

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18 298-102

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

TESTING AND EVALUATION OF SHIPBOARD WIRELESS NETWORK COMPONENTS

Richard J. McConnell
Lieutenant, United States Navy
B.S., Norfolk State University, 1993

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
March 2000

Author: ______________________
Richard J. McConnell

Approved by: ______________________
Xiaoping Yun, Thesis Advisor

____
Herschel H. Loomis, Second Reader

____
Jeffrey B. Knorr, Chair
Department of Electrical and Computer Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Fundamental challenges facing program managers and information technology decision makers today are the identification of architectures and technologies that reduce the cost of maintaining computer networks while simultaneously increasing worker productivity. Advances in wireless communications and subsequently, wireless local area networks (WLANs) permit mobile users to share information without being hardwired to a network. These mobile devices will enable shipboard personnel to submit damage control reports, update equipment logs, view technical manuals and order repair parts, without being confined by the limitations of a wired network. The advantages of WLANs are virtually endless, ranging from the uses previously discussed, to communications between the ship and its small boats, to automated data transfer of degaussing results, and even direct parts ordering from a pier-side supply center.

This thesis provides a hardware analysis and discusses coverage limitations of commercially available WLAN components for use onboard naval vessels. Utilization of this mobile equipment will improve DC communications and watchstander productivity. With remote access to the wired network backbone, personnel can conduct transactions instantaneously whenever and wherever the need arises. A discussion of the theories and principles governing the operation of WLANs is presented, followed by a laboratory evaluation of current, commercially available components.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF SYMBOLS, ACRONYMS AND/OR ABBREVIATIONS

λ	Wavelength
ACK	Acknowledgement
AP	Access Point
ASCI	Accelerated Strategic Computing Initiative
BDPSK	Binary Differential Phase Shift Keying
BPSK	Binary Phase Shift Keying
BRAN	Broadband Radio Access Networks
BSS	Basic Service Set
CAC	Channel Access and Control
CCA	Clear Channel Assessment
CCK	Complementary Code Keying
CCSK	Cyclic Code Shift Keying
CDMA	Code Division Multiple Access
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CTS	Clear to Send
dB	Decibels
DBPSK	Differential Binary Phase Shift Keying
DC	Damage Control
DCC	Damage Control Central
DECT	Digital European Cordless Telecommunications
DIFS	Distributed Inter Frame Space
DQPSK	Differential Quadrature Phase Shift Keying
DSSS	Direct Sequence Spread Spectrum
EIFS	Extended Inter Frame Space
ETSI	European Telecommunications Standards Institute

EY-NPMA	Elimination-Yield Non-Preemptive Multiple Access
FCC	Federal Communications Commission
FDMA	Frequency Division Multiple Access
FFH	Fast Frequency Hopping
FHSS	Frequency Hopping Spread Spectrum
FTP	File Transfer Protocol
GFSK	Gaussian Frequency Shift Keying
GMSK	Gaussian Minimum Shift Keying
HIPERLAN	High Performance Radio Local Area Network
HR	High Rate
HR/DSSS	High Rate Direct Sequence Spread Spectrum
Hz	Hertz
IEEE	Institute of Electrical and Electronic Engineers
IFS	Inter Frame Space
IP	Internet Protocol
IR	Infrared
ISM	Industrial, Scientific, and Medical
ISO	International Organization for Standardization
LAN	Local Area Network
LEO	Low Earth Orbit
LLC	Logical Link Control
LNA	Low Noise Amplifier
LOS	Line-of-Sight
LWCS	Light Wireless Communications System
MAC	Medium Access Control
MKK	Radio Equipment Inspection and Certifications Institute
MOK	M-ary Orthogonal Keying
MWWL	Millimeter Wave Wireless LAN
NLOS	Non-Line-of-Sight

NPS	Naval Postgraduate School
NSSN	New Attack Submarine
OCDM	Orthogonal Code Division Multiplexing
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
PHY	Physical Layer
PIFS	Point Coordination Inter Frame Space
PLCP	PHY Convergence Procedure
PLW	PSDU Length Word
PMD	Physical Media Dependent
PMS	Preventive Maintenance System
PN	Pseudo-Random Noise
PPM	Pulse Position Modulation
PSDU	PHY Service Data Unit
PSF	PLCP Signaling Field
QAM	Quadrature Amplitude Modulation
QDPSK	Quadrature Differential Phase Shift Keying
QPSK	Quadrature Phase Shift Keying
RAM	Random Access Memory
RF	Radio Frequency
RTS	Ready to Send
SFD	Start Frame Delimiter
SFH	Slow Frequency Hopping
SIFS	Short Inter Frame Space
SLN	Signal Level Number
SNR	Signal-to-Noise Ratio
SPDCS	Small Power Data Communication System
SR	Stored Reference
SYNC	Synchronization

TDMA	Time Division Multiple Access
TFLOPS	Trillion Floating Point Operations per Second
UMTS	Universal Mobile Telecommunications System
U-NII	Unlicensed National Information Infrastructure
W	Watt
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network

ACKNOWLEDGEMENTS

The author would like to acknowledge the financial support of the New Attack Submarine Program, PMS450T2, and the Naval Sea Systems Command in sponsoring the research involved.

The author would like to thank Professors Xiaoping Yun and Herschel Loomis for their direction during this research effort. Additional thanks is extended to my wife, Ana, and children, Alyssa and Alexander, for their steadfast patience and thoughtfulness.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Increasing worker productivity has been a driving force behind many advances in computer technology. Reduced size, increased speed and lower cost have all been key concepts in the development of devices that are designed to make our lives easier. The latest concept, wireless digital communications, is one that may possibly have the most profound impact on our day-to-day life and is the subject of this thesis. From the very beginning of time man has discovered that the use of simple machines would greatly decrease his workload. Today the concepts are quite the same but the technology is vastly different.

The computer age has allowed man to significantly decrease his workload and increase productivity. From the invention and enduring impact of the ENIAC, activated at the University of Pennsylvania over 50 years ago to one of the world's most powerful supercomputers of today, Intel's Accelerated Strategic Computing Initiative (ASCI) Option Red Supercomputer (also known as the Intel TFLOPS supercomputer) which is capable of executing at a rate of several trillion floating point operations per second (TFLOPS), many complex calculations and operations have been executed that would not have been completed otherwise. The Navy, much like the commercial industry, is continuously searching for ways to increase productivity of the individual, especially today with lower manning levels and the increased demand on our sailors. Utilization of computers has been an answer in the past and will continue to be the basis of future improvements.

The remarkable performance of the Smart Ship Program has unequivocally proven that the latest advances in technology can benefit the Navy enormously. The Smart Ship concept has demonstrated that shipboard workload reductions are possible while maintaining combat readiness and safety [Ref. 1]. Expenditures on available technology and implementation of policy and procedure changes are offset by large potential savings in manpower, both shipboard and ashore, and in operations and maintenance costs aboard ship. We have automated processes that in the past have required constant, round-the-clock monitoring, accounting for countless man-hours being wasted. Remote sensing devices and highly developed control systems perform tasks that are too difficult and often too dangerous for humans. It seems only logical that this next step in technology is one that will allow us to perform these operations with remote access without the limitations of physical connections. Recent advances in commercially available wireless networking components have made this option much more feasible and attractive for use onboard naval ships. These newer components now offer greater flexibility, increased range, higher data rates and interoperability between vendors. Presently the WLAN is not a substitute for the wired infrastructure but a consequential complement to what currently exists.

This thesis is part of a continuing analysis that investigates the plausibility and suitability of implementing wireless networks onboard naval vessels. Previous works supporting this project include theses by Debus [Ref. 2], Rothenhaus [Ref. 3], and Matthews [Ref. 4]. This thesis will focus on the comparison of commercially available radio frequency components for wireless networks that operate on the principle of direct sequence spread spectrum modulation.

A. MOTIVATION: WHY WIRELESS?

Hundreds of millions of people exchange information daily using pagers, cellular telephones, and other wireless communication products. Wireless technology now reaches virtually every location on the face of the earth. With the enormous success of wireless telephony and messaging services, it is hardly surprising that wireless communication is being applied to the realm of personal and business computing. No longer bound by the harnesses of wired networks, people are able to access and share information on a global scale nearly anywhere on the planet. Recent expeditions to the summit of Mt. Everest have even utilized wireless technology to relay up to the minute information back from the "roof of the world." Wireless LANs are a close cousin of the wired Ethernet or Token Ring networks that today, are ubiquitous in many computer environments. The wireless alternative simply uses radio frequency (RF) data transmission techniques vice signals transmitted via wire connections.

Since the success of the Ethernet project at Xerox's Palo Alto Research Center in the early 1970s and other similar digital protocols, the basic technology has been in place for local area networks (LANs) to blossom in both the public and private sectors. Standard LAN protocols, such as Ethernet, that operate at fairly high speeds with inexpensive connection hardware can bring digital networking to any computer. Today, organizations of every size access and share information over a digital network. However, until recently, LANs were limited to the physical, hard-wired infrastructure of a building. Even with phone dial-ups, network nodes were limited to access through wired, landline connections.

Many network users, especially mobile users in commercial businesses, the medical profession, factories, and universities, find benefit from the added capabilities of wireless LANs.

The major motivation and benefit from wireless LANs is increased mobility. Untethered from conventional network connections, network users can move about almost without restriction and access LANs from nearly anywhere. In addition to increased mobility, wireless LANs offer increased flexibility. One can visualize without too much difficulty, a meeting in which employees use mobile computing devices and wireless links to share and discuss future plans and products. This "ad hoc" network can be brought up and torn down in a very short time, either around the conference table or around the world. Wireless LANs offer the connectivity and the convenience of wired LANs without the need for expensive wiring or rewiring. [Ref. 5]

B. THE WIRELESS NAVY

By the sheer nature of the fact that ships have limited personnel assets it becomes imperative that the productivity of each crewmember be maximized. The NAVSEA New Attack Submarine (NSSN) program identified several areas for productivity improvement by deploying wireless local area networks (WLANs) and mobile computing devices onboard submarines. Specifically, these areas included damage control (DC) and watchstander logs. Accurate and timely communications between Repair Lockers, Damage Control Central (DCC) and the casualty scene have always been of utmost importance when combating shipboard casualties. Existent communication practices are cumbersome,

inefficient and ladened with opportunities for human errors. The current practice of watchstander log taking has similar needs for improvement.. Equipment logs are taken on locally generated paper forms, reviewed and eventually filed away. Rarely is there any correlation analysis conducted between daily collected logs. The biggest problem with this procedure is it doesn't lend itself well to trend analysis. The productivity in these and other areas could be greatly improved with the use of wireless networks and mobile computing devices. [Ref. 6]

It is very easy to see that once the gap between wired and wireless is bridged there would be countless other areas where productivity could be improved by use of wireless networks. Advances in wireless communications and subsequently WLANs permit mobile users to communicate with each other, access databases and share information without the need of being hardwired to the network. These mobile devices can be used by shipboard personnel to submit DC reports, update equipment operation logs, view technical manuals, access preventive maintenance system (PMS) documents and even order repair parts without being confined by the limitations of a wired network. A central database could be maintained where watchstanders make equipment log entries utilizing a handheld computer and wirelessly transmit the information for trend analysis. This database would allow multiple supervisors to review equipment performance in parallel and make decisions about equipment operations based on real-time data. From the uses previously discussed to communications with the ship's small boats to automated data transfer of degaussing results upon completion of a degaussing run to direct parts ordering through a wireless connection to a pier-side supply center, the advantages are virtually endless.

C. HOW WLANs WORK

Wireless LANs use electromagnetic waves to communicate information from one point to another without relying on physical connections. Radio waves are often referred to as radio carriers because they perform the function of delivering energy to a remote receiver. The data being transmitted is superimposed on the radio carrier so that it can be accurately extracted at the receiving end. This is generally referred to as modulation of the carrier by the information being transmitted. Multiple radio carriers can exist in the same space at the same time without interfering with each other if the radio waves are transmitted on different frequencies. To extract data, a receiver tunes in (or selects) one radio frequency while rejecting all other signals on different frequencies. In a typical WLAN configuration, a transmitter/receiver (transceiver) device, called an access point (AP), connects to the wired network from a fixed location using a standard Ethernet cable. At a minimum, the access point receives, buffers, and transmits data between the WLAN and the wired network infrastructure [Ref. 7]. The AP arbitrates access to the remote wireless stations by means of packetized data.

Most wireless LAN systems use spread-spectrum technology, a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. Spread-spectrum is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the tradeoff produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the

spread-spectrum signal being broadcast. If a receiver is not tuned properly, a spread-spectrum signal looks like background noise [Ref. 8]. The type of spread spectrum implementation stands out as the most significant characteristic of any LAN product. Generally speaking, radio LANs in the Industrial, Scientific, and Medical (ISM) bands either use direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS) techniques.

New forms of network access protocols are needed for proper operation of wireless networks. The Institute of Electrical and Electronic Engineers (IEEE) 802.11 standard governs the characteristics of wireless networking components. The IEEE 802.11 standard specifies Carrier Sense Multiple Access with collision avoidance (CSMA/CA) as the fundamental access method. CSMA/CA works by a "listen before talk scheme." This means that a station wishing to transmit must first sense the radio channel to determine if another station is transmitting. If the medium is available, the transmission may proceed.

The CSMA/CA scheme implements a minimum time gap between frames from a given user. Once a frame has been sent from a given transmitting station, that station must wait until the time gap is up to try to transmit again. Once the time has passed, the station selects a random amount of time (called a back-off interval) to wait before "listening" again to verify a clear channel on which to transmit. If the channel is still busy, another back-off interval is selected that is less than the first. This process is repeated until the waiting time approaches zero and the station is allowed to transmit. This type of multiple access ensures judicious channel sharing while avoiding collisions.

CSMA/CA allows automatic medium sharing between several devices with compatible physical layers. This access method is attractive because it provides spectral efficiency as well as asynchronous data transfer. Frequency Division Multiple Access (FDMA) and Code Division Multiple Access (CDMA) schemes would not be adequate because they require bandwidth used by the modulation scheme. Strict Time Division Multiple Access (TDMA) would not work well because it requires synchronization. Thus CSMA/CA, which may be thought of as a version of TDMA, is better suited to this application. [Ref. 9]

Roaming is one of the main advantages of a wireless network, allowing users to freely move about while maintaining connectivity. A single access point can support a small group of users. The access point (or the antenna attached to the access point) is usually mounted high but may be mounted essentially anywhere that is practical as long as the desired radio coverage is obtained. End users access the WLAN through wireless LAN adapters, which are implemented as PC cards in notebook computers, or use ISA or PCI adapters in desktop computers, or fully integrated devices within hand-held computers. WLAN adapters provide an interface between the client network operating system and the airwaves (via an antenna). The nature of the wireless connection is transparent to the network operating system since the details of the transmission is handled by the Medium Access Control (MAC) and Physical layers of the Open Systems Interconnection (OSI) model illustrated in Fig. 1.1. [Ref. 7]

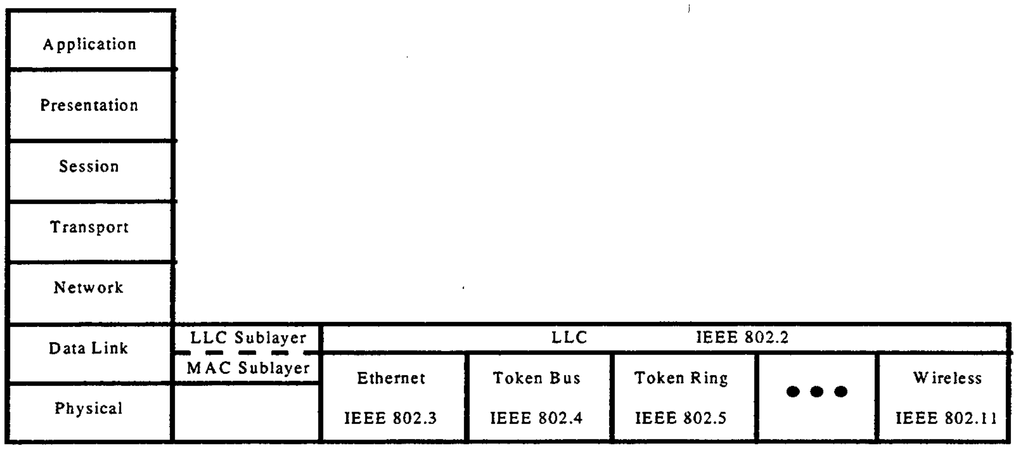


Figure 1.1: OSI Model From Ref. [10]

D. BENEFITS

The dependence on networking among businesses and the meteoric growth of the Internet and online services are strong testimonies to the benefits of shared data and shared resources. With wireless LANs, users can access shared information without looking for a place to plug in, and network managers can set up or augment networks without installing or moving wires. Wireless LANs offer the following productivity, service, convenience, and cost advantages over traditional wired networks:

- Mobility - WLANs can provide users with access to real-time information anywhere in their organization. Mobility supports productivity and service opportunities not possible with wired networks.
- Installation Speed and Simplicity - Installing a WLAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.
- Installation Flexibility - Wireless technology allows the network to go where wire cannot go.

- Reduced Cost-of-Ownership - While the initial investment required for WLAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves, additions, or changes.
- Scalability - WLAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks to full infrastructure networks of thousands of users that allow roaming over a broad area. [Ref.11]

E. GOAL FOR THIS THESIS

The goal of this thesis is to evaluate several commercially available wireless components that operate on the principal of direct sequence spread spectrum (DSSS). A comparative analysis will be conducted between several wireless components to include a comparison between line-of-sight (LOS) and non-line-of-sight (NLOS) performance. The analysis will also include a comparison between the IEEE (Institute of Electrical and Electronics Engineers) 802.11 compliant 1- and 2-Mbps data rate components and the newest version operating at a data rate of 11 Mbps.

F. THESIS OUTLINE

This thesis is organized as follows. Chapter II discusses background information presented in a previous thesis by Matthews [Ref. 4]. Chapter III presents a brief analysis of the IEEE 802.11 standard for Wireless LAN Medium Access Control (MAC) and Physical

Layer specifications. Next, Chapter IV discusses the principles of spread spectrum modulation and provides a comparison between direct sequence and frequency hoping techniques. Both are viable choices of spread spectrum implementations and both have been field proven. Chapter V presents the results of the laboratory testing and determines which of the components evaluated offers the most promising performance for the shipboard wireless networking needs of the Navy. In conclusion, Chapter VI summarizes the results and investigates the suitability of implementing wireless networks onboard naval vessels.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

This chapter is a summary of the information presented in a thesis by Matthews [Ref. 4]. This background information provides a crucial look at the various options available in wireless technology and forms a basis for continued research in the area of wireless local area networks.

A. IMPACTS ON SIGNAL PROPAGATION

The most basic model of radio wave propagation involves so called "free space" radio wave propagation. In this model, radio waves emanate from a point source of radio energy, traveling in all directions in a straight line, filling the entire spherical volume of space with radio energy that varies in strength with a $1/(\text{range})^2$ rule. Real world radio propagation rarely follows this simple model. The three basic mechanisms of radio propagation are attributed to reflection, diffraction and scattering. All three of these phenomenon cause radio signal distortions and give rise to signal fades, as well as additional signal propagation losses.

With mobile units, movements over very small distances give rise to signal strength fluctuations, because the composite signal is made up of a number of components from the various sources of reflections (called "multipath signals") from different directions as well as scattered and / or diffracted signal components. In the real world, multipath occurs when there is more than one path available for radio signal propagation. The phenomenon of

reflection, diffraction and scattering all give rise to additional radio propagation paths beyond the direct optical "line of sight" path between the radio transmitter and receiver.

1. Reflection

Reflection occurs when a propagating electromagnetic wave impinges upon an object which has very large dimensions when compared to the wavelength (λ) of the propagating wave. Reflections occur from the surface of the earth and from buildings and walls.

2. Diffraction

Diffraction occurs when the radio path between the transmitter and receiver is obstructed by a surface that has sharp irregularities (edges). The secondary waves resulting from the obstructing surface are present throughout the space and even behind the obstacle. Diffraction is the phenomenon responsible for the RF energy traveling between the transmitter and receiver without a line-of-sight path does not exist between transmitter and receiver. This occurrence is often referred to as shadowing because the diffracted signal can reach the receiver even though an impenetrable object shadows it. At high frequencies, diffraction, like reflection, depends on the geometry of the object, as well as the amplitude, phase, and polarization of the incident wave at the point of diffraction.

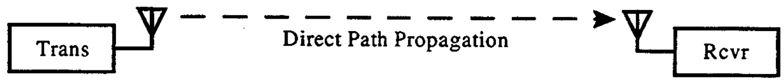
3. Scattering

Scattering occurs when the medium through which the wave travels consists of objects with dimensions that are small compared to the wavelength, and where the number of obstacles per unit volume is large. Scattered waves are produced by rough surfaces,

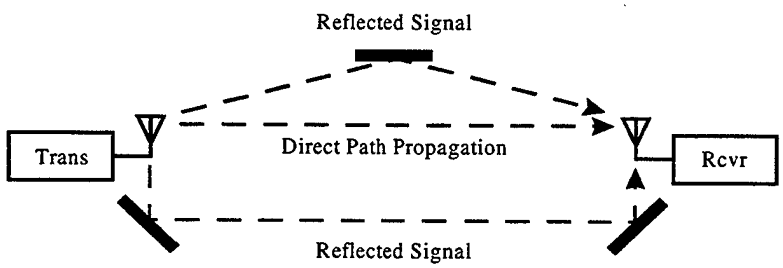
small objects, or by other irregularities in the channel. In practice, foliage, street signs, and lampposts induce scattering in a mobile communications system. When the wave impinges on either a large rough surface or any surface whose dimensions are on the order of λ or less the reflected energy to spread out (scattered) in all directions. [Ref. 12]

B. CHARACTERISTICS OF THE SHIPBOARD RF CHANNEL

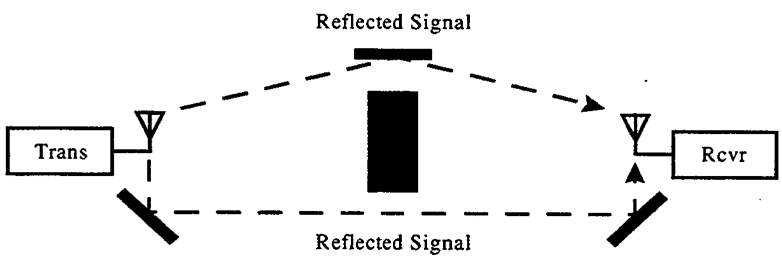
There are many impediments onboard naval ships that preclude direct path propagation and heighten multipath signal propagation. In a wireless mobile communication system, a signal can travel from the transmitter to the receiver over multiple paths. These paths can be either direct or reflected. This phenomenon is known as multipath propagation. Multiple reflective paths cause fluctuations in the received signal's amplitude, phase and angle of arrival. This occurrence gives rise to the term multipath fading and refers to a signal's random fluctuations or fading due to multipath propagation [Ref. 13]. Figure 2.1 illustrates typical geometries that produce different signal path receptions. The presence of the multipath components greatly degrades channel performance and complicates analysis. In a shipboard environment direct path propagation rarely exists and because Rayleigh fading channels offer worst-case performance, the shipboard RF channel is characterized as a Rayleigh fading channel.



a. Direct Path Reception (AWGN)



b. Multipath Reception with Direct Path Component (Ricean)



c. Multipath Reception without Direct Path Component (Rayleigh)

Figure 2.1: Channel Reception Path Models

C. RAYLEIGH FADING CHANNELS EFFECTS

Fading channels affect signal propagation in several ways. The basic signal attenuation with range noticed in the real world gives rise to what are termed "large scale" effects, while the signal strength fluctuations with motion are termed "small scale" effects.

1. Large-Scale Fading

Large-scale fading is predominately dependent upon the terrain of the region between the transmitter and receiver and provides a means to account for the signal attenuation due to obstructions. While large-scale fading causes degradation of signal reception, it is easily countered by including an approximation of expected or worst-case large-scale fading attenuation in the link budget analysis to mitigate its effects.

2. Small-Scale Fading

Small-scale fading refers to the dramatic changes in signal amplitude and phase that can be experienced as a result of small changes in spatial separation between a receiver and transmitter. Small-scale fading is also called Rayleigh fading because if there is a large number of multiple reflective paths and no line-of-sight component, the envelope of the received signal is statistically described by a Rayleigh probability density function. On the other hand, if there exists a dominant nonfading signal component, such as a line-of-sight propagation path, the small-scale envelope is described by a Ricean probability density function. Small-scale fading manifests in two forms: time spreading of the signal (signal dispersion) and time variance of the channel. [Ref. 13]

a) Time Spreading of the Signal

Each multipath reception experiences a different delay time causing a time spreading of the received signal. The channel is said to experience flat fading as long as the multipath receptions occur during the duration of the transmitted symbol.

b) Time Variation of the Channel

The time-varying nature of the channel is caused by the relative motion between the transmitter and receiver, or by movement of objects within the channel. The channel is time-variant because motion between the transmitter and the receiver causes the propagation paths of the multipath receptions to change. This results in variations in the received signals amplitude and phase.

D. SHIPBOARD RF CHANNEL CLASSIFICATION

With an analysis of selected communications systems, it is easy to determine if the channel will exhibit frequency selective or flat fading. Due to the compartmentalization of the shipboard environment, it can be assumed that all channel receptions will essentially occur within one symbol period and the channel will exhibit flat fading characteristics. These characteristics are largely dependent upon the geometry between the transmitter and receiver. A slowly moving transmitter and receiver, compared to the symbol rate, should produce a slowly varying channel. The shipboard RF channel should, therefore, exhibit slow fading characteristics.

E. RESISTING FADING CHANNELS

Given that the communication channel exhibits flat, slowly fading characteristics, efforts to improve system performance focus on mitigation of the effects of the deep fading phenomenon. The most prominent method used to minimize susceptibility to deep fading is spread spectrum modulation.

F. SPREAD SPECTRUM SYSTEMS IN ISM BANDS

In 1985 the Federal Communications Commission (FCC) issued the Part 15 Rules which permitted unlicensed use and development of spread spectrum communications systems in the ISM bands. Many spread spectrum products have been introduced to the consumer market. In order to promote multi-vendor compatibility, the Institute of Electrical and Electronic Engineers (IEEE) has issued the IEEE 802.11 standard, governing the characteristics of wireless networking components.

G. FREQUENCY-HOPPING SPREAD SPECTRUM TECHNOLOGY

FHSS uses a narrowband carrier that changes frequency in a pattern known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise [Ref. 8]. A FHSS communications system can be implemented by periodically varying the carrier frequency of a narrowband system. FHSS systems can be categorized as either fast frequency hopping (FFH) or slow frequency hopping (SFH) depending upon the relationship between the period of the carrier frequency variation and the period of the transmitted symbol.

If the carrier frequency changes more rapidly than the transmitted symbol, the system is a FFH system. Each symbol is subsequently transmitted over multiple carrier frequencies with the signal between the carrier frequency hops referred to as a chip. If the difference in carrier frequencies exceeds the coherence bandwidth of the channel, each chip is received independently, providing a form of frequency diversity. If a chip is transmitted

with a carrier frequency affected by a deep fade in the multipath channel, the receiver may still be able to reconstruct the symbol based upon the reception of the other independent chips. On the other hand, SFH systems provide no protection against deep fading. As the carrier frequency changes at a rate less than the symbol rate, many symbols are transmitted during each chip. As a result, many symbols are lost when the carrier frequency lies in a deep fade region of the spectrum.

H. DIRECT-SEQUENCE SPREAD SPECTRUM TECHNOLOGY

Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called the spreading or chipping code. The longer the chip, the greater the probability that the original data can be recovered and the more bandwidth required. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low-power wideband noise and is rejected (ignored) by most narrowband receivers. [Ref. 8]

A DSSS system is implemented by modulating a narrowband signal with a bipolar chipping code that is generated by a pseudo-noise (PN) generator. At the receiver, the DS modulation is removed by, again, applying the chipping code modulation. In order for a successful reception in a DSSS system, the PN generator at the transmitter and receiver must be synchronized.

DSSS systems that are compliant with the initial IEEE 802.11 standard transmit at a rate of 1 Mbps or 2 Mbps in the 2.4 GHz range of the ISM band. The higher data rate

utilizes quadrature differential phase shift keying (QDPSK) modulation while the lower rate uses binary DPSK (BDPSK) modulation.

I. DSSS AND FHSS COMMONALTIES

Before we address the differences in wireless LAN implementations we should first consider the commonalties. First of all, the products must work on the same frequency bands. Because the 2.4-GHz band is available virtually worldwide, most vendors are concentrating new wireless LAN efforts on that band. A second commonality is that both share the IEEE 802.11 standard, which ensures interoperability among vendors. Despite sharing the spread spectrum name, DSSS and FHSS could hardly be less similar. DSSS systems broaden the signaling band by artificially increasing the modulation rate using a spreading code. FHSS systems, meanwhile, hop from narrow band to narrow band within a wide band, using each narrow band for a specific time period. The frequency hops appear random although they actually occur in a pseudo-random sequence tracked by the sender and receiver. [Ref. 14]

J. FREQUENCY HOPPING VS. DIRECT SEQUENCE

Having set the stage, FHSS and DSSS systems can now be compared relative to the following characteristics that effect performance: Coverage and Reliability, Immunity to Impairment, Scalability, and Room for Growth.

1. Coverage and Reliability

In general DSSS systems offer a receiver sensitivity advantage that results in a greater range and a more reliable link. In fact, coverage area in a wireless LAN is determined by a combination of three factors – total output power, signal to noise ratio (SNR), and total receiver noise level. The third factor is normally independent of DSSS and FHSS implementations, since it is mainly based on the noise introduced in the first stage of the receiver (RF-input stage: filter and gain stages) and/or the environmental noise, whichever is stronger. The same environmental noise level applies for both systems. Therefore total receiver noise is not important for the purpose of this comparison.

Governmental regulations can play a role in the transmit power component of range. The Federal Communications Commission (FCC) allows either DSSS or FHSS systems to use 1 Watt or less. Actually other practical considerations prove more important in determining transmit power. Both DSSS and FHSS implementations must support the PCMCIA form-factor used in portable, battery-powered systems. These implementations provide a transmit power in the 50-100 mW range. These devices must deal both with current consumption limits not only in transmit mode, but also in receive mode. In practice, transmit power is limited by the amount of current that can be drawn from the PCMCIA slot, rather than the regulatory power constraint. The practical limitations on transmit power mean that SNR differences in the DSSS and FHSS largely determine differences in range. The difference between DSSS and FHSS in the allowable path loss between transmitter and receiver, is dominated by the difference in the minimum required SNR. The

QPSK modulation used in DSSS systems yields a 4 to 10 dB SNR advantage relative to FSK modulation in FHSS. The SNR advantage translates into a 50% advantage in coverage area for a DSSS system operating at the same bit rate and transmit power as a FHSS system. [Ref. 14]

2. Immunity to Impairments

FHSS and DSSS systems combat frequency-selective fading in different ways and both are effective. FHSS systems simply retransmit the same information a second time at the next hop frequency when fading disrupts a transmission. A DSSS receiver, meanwhile, integrates the signal across a much wider spectrum. The receiver can, therefore, operate with low responses in part of the spectrum with no need for retransmission. These spread spectrum systems work similarly, specifically in a region of narrowband interference created by deep fade regions. Most FHSS systems are implemented using SFH modulation. Instead of providing protection against deep fade regions of the multipath environment, these FHSS systems rely on the probability that most of their transmitted frequencies will occupy flat-fading regions of the channel spectrum. The symbols that are transmitted in deep fade channels will be retransmitted after the carrier hops to an unaffected frequency. On the other hand, the DSSS signal is spread so that the demodulated received signal will be virtually unaffected by deep fade regions of the multipath environment. This increase in interference resistance is gained through the sacrifice of bandwidth efficiency. Both systems can recover, but FHSS systems suffer a slight degradation in performance due to retransmission.

3. Scalability

Scalability refers to the ability to physically collocate multiple FHSS or DSSS systems without generating mutual interference, which could render adjacent channels unusable. For DSSS, acceptable performance is achieved with three collocated channels operating with 25 MHz of separation. Thus, no more than three collocated DSSS systems are feasible for the 2.4 GHz frequency portion of the ISM band. FHSS systems offer a more efficient use of the allocated bandwidth. While the IEEE 802.11 standard calls for 79 channels, the mutual interference becomes unacceptable if more than fifteen channels are collocated. While it seems safe to assume that the aggregate throughput of the fifteen collocated FHSS systems would exceed that of three collocated DSSS systems, this is not necessarily the case. It has been reported that FHSS aggregate performance peaks with thirteen collocated IEEE 802.11 compliant systems offering less total throughput than three collocated IEEE 802.11 compliant DSSS systems. Due to the inherent robustness of the DSSS signal, direct sequence systems using the same channel can be placed closer together than frequency hopping systems.

4. Room for Growth

FHSS systems are severely limited by the utilization of FSK modulation. The 1 MHz channel bandwidth required by the FCC Part 15 rules allows only BFSK or QFSK modulation. The data rate gain achieved by increasing the number of bits per symbol is restricted by compliance with the maximum channel bandwidth limitation. DSSS systems utilize the more bandwidth efficient PSK modulation where the bandwidth does not

increase with signal complexity. Thus, greater data rates can be achieved by utilizing more bits per symbol at the expense of an increase in transmit power or a decrease in range.

K. WIRELESS NETWORKING AND THE IEEE 802.11 STANDARD

To aid in developing networking systems components that enable diverse computing systems to communicate and share data, the International Standards Organization developed the Open System Interconnection (OSI) model illustrated in Fig. 1.1. The figure also shows that specific network protocols such as Ethernet or Token Ring are implemented in the two lowest layers of the OSI model: the data link layer and the physical layer. The services provided by the upper layers of the model are independent of the network implementation. Wireless components performing the functions of the data link layer and the physical layer of the OSI model enable network members to function without physical connections.

The lowest layer of the OSI model, the physical layer, governs the transmission media and the transmitted signal. The transmission media may consist of a guided medium such as twisted pair, coaxial cable, or optical fibers or the media may be unguided as in the case of radio wave, microwave, or infrared links. The physical layer also defines the voltage levels used to represent the transmitted data values for guided media.

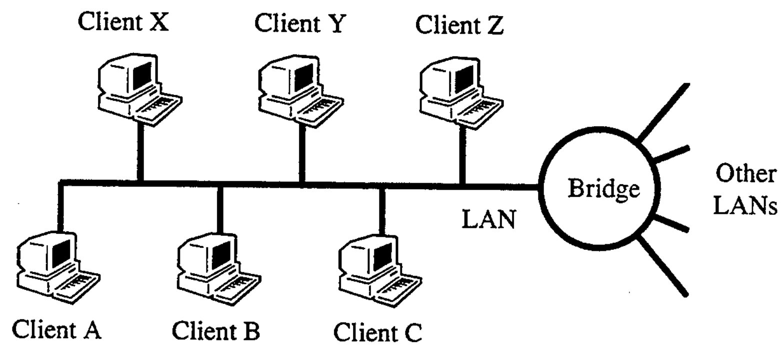
The data link layer, the second layer in the OSI model, can be subdivided into two parts: the Medium Access Control (MAC) and the Logical Link Control (LLC) sublayers. Because most networks use a shared media where multiple transmitters are connected to the same transmission channel, a MAC protocol must be used to prevent multiple transmitters from sending data simultaneously. Medium access in the Ethernet protocol is controlled

using a carrier-sense multiple access with collision detection (CSMA/CD) algorithm. Token Ring networks avoid data collisions by allowing only the station currently possessing the data token to transmit. The LLC sublayer provides error control and flow control for the network connection. The error control algorithm attempts to detect and correct or discard errors in received data. The flow control aspects of the LLC sublayer controls the transmission and acknowledgment of data frames.

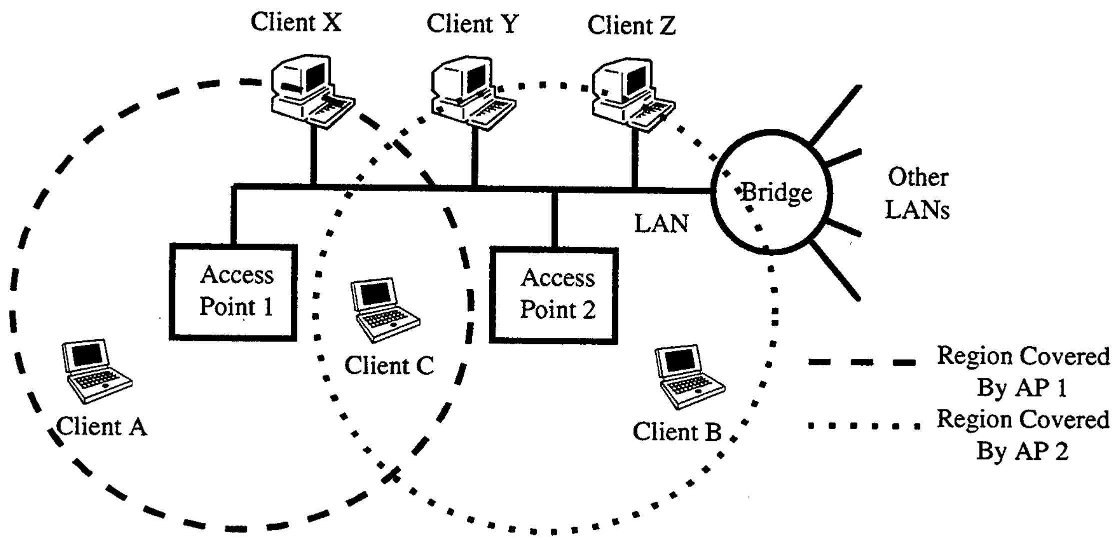
Simply replacing the physical layer aspects of networking components with radio transmitters will not produce a wireless network. Figure 2.2a shows a topographical diagram of a typical bus oriented LAN. Each client is connected to the network by a physical link, typically twisted pair, coaxial cable, or optical fiber. Figure 2.2b shows a similar network utilizing both wired and wireless connections. Clients X, Y, and Z are still physically connected to the network bus but clients A, B, and C are connected to the network through radio frequency links with access points (APs). APs pass data packets between their wireless clients and the guided distribution component of the network. Figure 2.2c shows a topography referred to as an ad-hoc wireless network. The clients of ad-hoc networks communicate only between themselves and are not connected with guided media. Each of the topographies shown in Fig. 2.2 differs only slightly in physical layout, but there are significant differences in how the clients of the network interoperate. In Fig. 2.2b it is clear that clients A and B communicate with the network through their respective APs. However, client C could be associated with either AP 1 or AP 2. Transmitting data to both APs would produce duplicated data on the network, degrading efficiency. Additionally, the wireless network shown in Fig. 2.2b must allow dynamic association between mobile

clients and the APs. As a mobile client roams from an area covered by one AP to another, the transition must appear seamless to the upper layers of the OSI model.

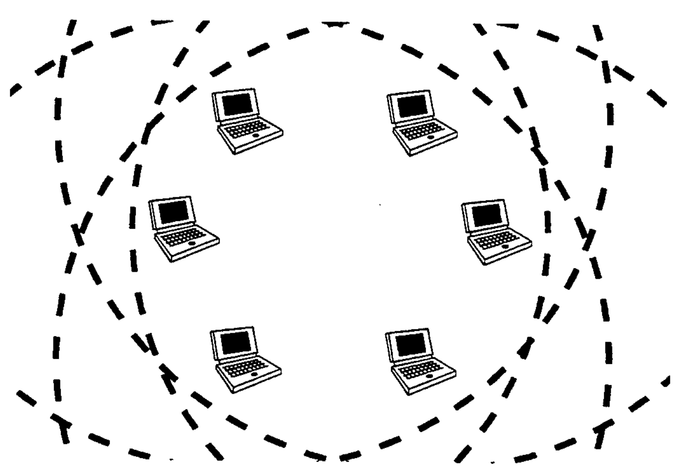
As shown in Fig. 1.1, specific network architectures are implemented in the lowest two layers of the OSI model. In fact, the physical layer and the MAC sublayer determine the architecture.



a. Conventional LAN



b. Infrastructure-Based WLAN



c. Ad-hoc WLAN

Figure 2.2: LAN Configurations

L. THE IEEE 802.3 STANDARD: CSMA/CD NETWORKS

While Ethernet is commonly used interchangeably with CSMA/CD or IEEE 802.3 LANs there are some differences. Therefore, the CSMA/CD network characteristics will be described, but these characteristics can be generally applied to networks commonly referred to as Ethernet LANs.

1. The Physical Layer

As shown in Table 2.1, the IEEE 802.3 standard specifies several physical media and signaling techniques. The most common form of the IEEE 802.3 LAN utilizes the 10BASE-T format. Although broadband signaling is permitted with 10BROAD36 implementations, most CSMA/CD LANs use baseband signaling with Manchester coding.

	10BASE5	10BASE2	10BASE-T	10BROAD36	10BASE-FP
Transmission Medium	Coaxial Cable	Coaxial Cable	Unshielded Twisted Pair	Coaxial Cable	Optical Fiber
Signaling Technique	Baseband (Manchester)	Baseband (Manchester)	Baseband (Manchester)	Broadband (DPSK)	OOK (Manchester)
Network Topology	Bus	Bus	Star	Bus/Tree	Star

Table 2.1: Description of IEEE 802.3 Physical Media

2. The MAC Sublayer

For IEEE 802.3 LANs medium access is governed by a CSMA/CD protocol. When a network client has data to transmit, it first attempts to determine if the channel is idle. If no transmissions are detected, the client will begin to transmit its data packet. If the medium is not idle, the client will wait until the channel is clear and then begin

transmission. Transmitted signals propagate at a finite speed dependent upon the transmission media, it is clear that this MAC protocol does not prevent data collisions. One network client could determine that the channel is idle and begin to transmit data. During the time required for signal propagation, another client could sense that the channel is idle and also begin to transmit data. A data collision or an overlapping of transmitted signals would occur.

When a transmitting client detects a data collision, it transmits a short jamming signal to ensure that all clients are aware of the collision. The clients affected by the data collision then enter a random back-off period, using a binary exponential back-off algorithm, prior to attempting to retransmit to minimize the probability of reoccurring collisions. After the initial collision occurs, the affected clients wait either zero or one time interval. If a second collision occurs then the clients will randomly wait zero, one, two, or three time intervals. The 802.11 standard for wireless networks is vastly different especially when dealing with hidden clients. A hidden client is one in which a distant client cannot detect its transmissions. A detailed explanation of the IEEE 802.11 standard will be presented in the following chapter.

M. RESULTS THUS FAR

Since this thesis is a continuation of research previously conducted, the results presented here are designed to give background information on the testing conducted to this point. The components tested and the testing procedures will be cover in detail in Chapter V.

DSSS components offer better performance than FHSS systems. The results of testing conducted on several commercially available, wireless networking components, indicate that the Lucent Technologies WaveLAN IEEE components offer the best performance of the selected devices. The coverage area provided by the WaveLAN IEEE components is larger and the throughput is higher compared to the other selected devices. The fact that DSSS components outperformed the FHSS components did not come as a surprise. First, recall that the DSSS components use PSK modulation, which is much more efficient than the FSK modulation used by FHSS components. The FHSS devices require a much higher SNR to achieve the same probability of bit error. Secondly, the DSSS components mitigate the effects of the deep-fade regions of the channel. Errors occur more rarely in DSSS systems because the signal energy is spread through a wider bandwidth. For FHSS systems, deep-fade regions of the channel periodically prevent successful transmissions. As the FHSS system changes frequencies after several hundreds of milliseconds, many packets must be retransmitted due to the multipath channel, thereby reducing overall efficiency.

THIS PAGE INTENTIONALLY LEFT BLANK

III. IEEE 802.11 STANDARD AND BEYOND

With the success of wired LANs, the market has moved toward a more attractive technology: developing wireless LANs (WLANs) with the speed of current wired LANs. Companies have developed WLAN systems which can provide data rates of 11 Mbps and higher. The higher data rates make WLANs a very promising technology for the future communications market.

There are several issues associated with WLANs:

- Error rate: For wired LANs, errors are relatively rare. But in the world of radio, error rate is much higher. Noise, multipath, attenuation, spread-spectrum interference, etc. are all common causes for errors in the wireless environment.
- Security: Radio waves are not confined at the boundary of buildings or compartments. There exists the possibility for eavesdropping and intentional interference.
- Interference: In a wired LAN, the only machines you hear are the ones connected to the network. In a WLAN you may hear other networks, as well as cordless phones, microwave ovens, etc. Any of these can interfere with data transmission. Physical obstructions also interfere with signal reception as illustrated in Fig. 3.1. This interference can either be constructive or destructive.
- Power conservation: WLANs are typically related to mobile applications, and in this type of application, battery power is a scare resource.

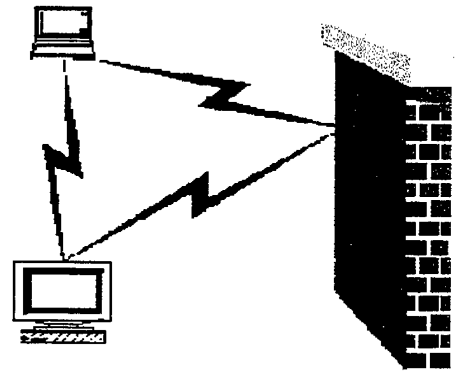


Figure 3.1: Multipath Interference From Ref. [15]

WLANs are typically designed to operate in the Instrumentation, Scientific, and Medical (ISM) radio bands. The ISM bands include frequency ranges of 902-928 MHz, 2.4-2.483 GHz, 5.15-5.35 GHz, and 5.725-5.875 GHz. [Ref. 15]

A. GLOBAL STANDARDIZATION EFFORTS

One of the major problems concerning wireless technology is standardization. The problems concerning standardization are, among other things, making the best use of a scarce resource, the radio spectrum, while at the same time making the standard attractive enough to use so the market can grow. A number of global and national standardization initiatives have taken place in wireless technology.

The global organization, IEEE had worked for 7 years on the 802.11 standard, which specifies to vendors how to implement the over-the-air interface for a wireless local area network. This standard accommodates both infrared and spread-spectrum radio with a protocol called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) which is similar to Carrier Sense Multiple Access with Collision Detection (CSMA/CD) used in the Ethernet. In the US a new standard, called NII/SUPERnet, has been introduced

which makes available 300 megahertz of spectrum at 5.15-5.35 GHz and 5.725-5.825 GHz bands for use by a new category of unlicensed equipment, called Unlicensed National Information Infrastructure ("U-NII") devices [Ref. 16]. Figure 3.2 is presented to show the availability of the 2.4 GHz band throughout the world.

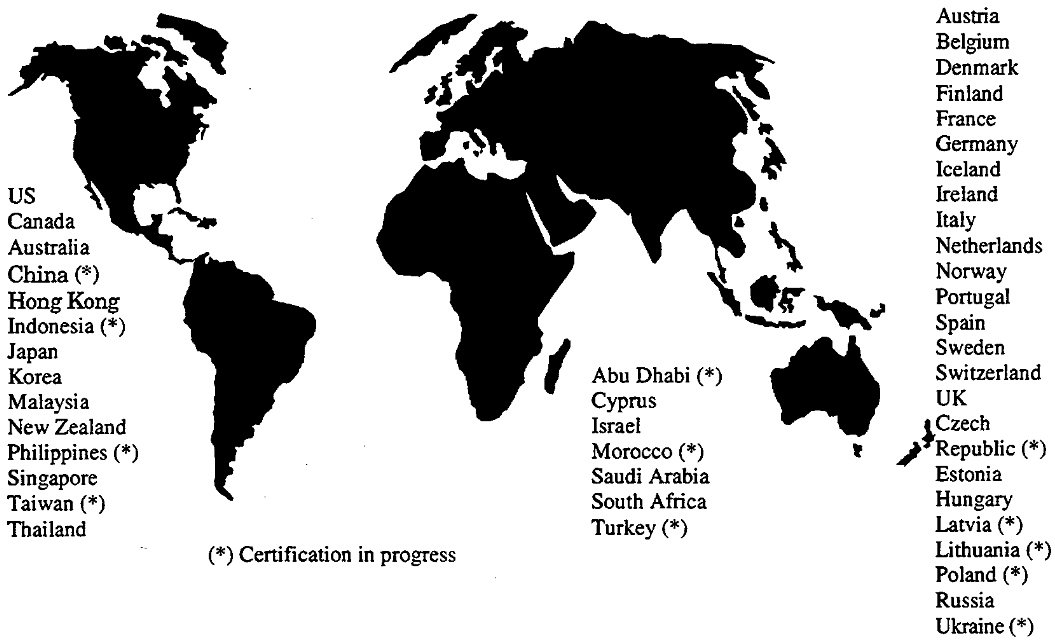


Figure 3.2: Availability of the 2.4 GHz Band After Ref. [17]

JAPAN has introduced the Small Power Data Communication System (SPDCS) standard, which operates at 2.4Ghz. JAPAN has also introduced standards in the 19 GHz spectrum - Light Wireless Communications System (LWCS) and in the 30-300 GHz spectrum - Millimeter Wave Wireless LAN (MWWL). Europe has introduced the Digital European Cordless Telecommunications (DECT) standard (which is not a LAN standard) and has recently introduced the HIPERLAN standard after several years of work.

The networking industry itself has taken an important initiative under the name of WLANA, whose members include 3Com, Aironet Wireless Communications, AMD,

Digital, Harris Semiconductor, IBM, Lucent Technologies, Proxim, and others. WLANA promises to promote increased awareness and knowledge of WLANs among potential customers, software vendors and systems integrators [Ref. 16].

B. INTRODUCTION TO THE IEEE 802.11 STANDARD

The IEEE 802.11 standard specifies a choice of three different physical layers (PHY), any of which can underlie a single medium-access control (MAC) layer. Members of the 802.11 working group felt that a choice of PHY implementations was necessary so that system designers and integrators could choose a technology that matches the price, performance, and operations profile of a specific application. These choices are exactly analogous to choices such as 10BaseT, 10Base2, and 100BaseT in the Ethernet arena. Moreover, enterprise LANs will regularly mix wired Ethernet and wireless nodes with no logical distinction between the two.

Specifically, the standard provides for an optical-based PHY that uses infrared light to transmit data, and two RF-based PHY that leverage different types of spread-spectrum radio communications as illustrated in Fig. 3.3. The infrared PHY will typically be limited in range and most practically implemented within a single room or compartment. The RF-based PHY can be used to cover a relatively large area. [Ref. 18]

The infrared PHY provides for 1-Mbps-peak data rates with a 2-Mbps rate optional and relies on pulse position modulation (PPM). The RF PHYs include Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS) choices. As the names imply, both DSSS and FHSS artificially spread the transmission band so that the

transmitted signal can be accurately received and decoded in the face of noise. The two RF PHYs, however, approach the spreading task in significantly different ways.

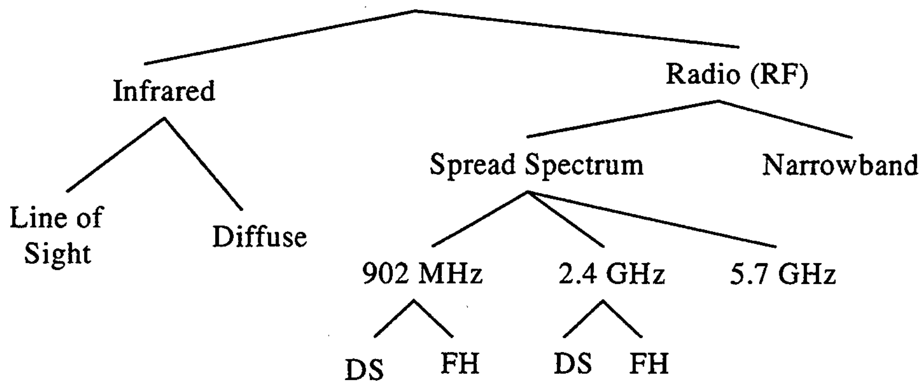


Figure 3.3: IEEE Physical Layer Provisions After Ref. [19]

FHSS systems essentially use conventional narrow-band data transmission techniques but regularly change the frequency at which they transmit. The systems hop at a fixed time interval within a wide band using different center frequencies in a predetermined sequence. The hopping phenomenon allows the FHSS system to avoid narrow-band noise in portions of the transmission band. As discussed in Chapter II, FCC Part 15 Rules define the operations of spread spectrum systems in the ISM bands.

The FCC placed the following restrictions on FHSS systems in the 2.4 GHz band:

- Maximum dwell time per hop: 400 msec
- Minimum number of hop channels: 75
- Maximum channel bandwidth: 1.0 Mhz

The standard defines the FHSS PHY to operate at 1 Mbps and allows for optional 2-Mbps operation. The FHSS PHY uses 2 or 4 level Gaussian frequency shift keying (GFSK) modulation.

DSSS systems artificially broaden the bandwidth needed to transmit a signal by modulating the data stream with a spreading code. The receiver can detect error-free data even if noise persists in portions of the transmission band.

The FCC placed the following restrictions on DSSS systems:

- Minimum spreading bandwidth: 500 kHz
- Minimum processing gain: 10dB

. In the United States the carrier frequency ranges from 2.412 GHz to 2.462 GHz depending upon which of the eleven channels is selected. Each channel is separated by 5 MHz. A more detailed analysis of FHSS and DSSS is presented in the following chapter.

In 802.11, the DSSS PHY defines both 1- and 2-Mbps peak data rates. The former uses differential binary phase shift keying (DBPSK) and the latter uses differential quadrature phase shift keying (DQPSK). [Ref. 18]

C. IEEE 802.11 COMMITTEE

The IEEE Standards Board approved the 802.11 standard for WLANs on June 26, 1997. The working group ratified the standard for WLANs operating at a maximum speed of 2 Mbps. The main features of the 802.11 standard are:

- robustness
- multi channel roaming
- power management
- automatic rate selection
- security

Since the approval of the standard, the IEEE 802.11 Working Group has been concentrating its efforts on producing standards for high-speed WLANs. Table 3.1 list the IEEE 802.11 family of standards.

	IEEE 802.11 (DSSS)	IEEE 802.11a	IEEE 802.11b
Application	Wireless Ethernet (LAN)	Wireless ATM	Wireless Ethernet (LAN)
Frequency	2.4 GHz	5 GHz	2.4 GHz
Data Rate	1-2 Mbps	20-25 Mbps	5.5 & 11 Mbps

Table 3.1: IEEE 802.11 Family of Standards After Ref. [15]

1. Modulation

The initial 802.11 compliant, DSSS WLAN systems use binary phase shift keying (BPSK) and quadrature phase shift keying (QPSK) modulation schemes. They are sufficient in 1 and 2 Mbps systems, but they do not meet the demands of higher data rate transmission schemes. To achieve higher speeds, different modulation techniques needed to be implemented. The possible techniques considered by the committee were:

- M-ary orthogonal keying (MOK)
- complementary code keying (CCK)
- cyclic code shift keying (CCSK)
- pulse position modulation (PPM)
- quadrature amplitude modulation (QAM)
- orthogonal code division multiplexing (OCDM)
- orthogonal frequency division multiplexing (OFDM)

The first addition to the 802.11 family was the 802.11a standard which governs a high-speed PHY in the 5 GHz ISM band that can be used with the existing 802.11 MAC layer specification and be suitable for the transport of not only data but voice and image. The 5 GHz ISM band will allow for speeds of 24 Mbps or higher. The 802.11a standard is based on OFDM to modulate the data. OFDM enables the utilization of wide band signals in an environment where reflected signals would otherwise disable the receiver from recovering the data from the received signal. The RF system operates in the 5.15-5.25, 5.25-5.35 and 5.725-5.825 GHz Unlicensed National Information Infrastructure (U-NII) bands. The OFDM system provides for data rates of 6-54 Mbps. Since there is such a similarity between the IEEE 802.11a and the HIPERLAN/2 standards, the two specifications essentially feature the same physical layer. [Ref. 15]

The second addition, 802.11b, manages a high-speed PHY extension in the 2.4 GHz band. The current 802.11 MAC layer provides for multiple data rates within the same area and allows for the computation of higher data rates, even by stations that may not support them. This means that stations could support a higher data rate and be backward compatible with existing products [Ref 15]. The IEEE 802.11b committee selected CCK, as proposed by Lucent Technologies and Harris Semiconductor, for the higher data rates in the 2.4 GHz band. CCK is a form of MOK modulation where the code symbols are four phase modulated. It supports both 5.5 Mbps and 11 Mbps modulation, and is backward compatible with the 1-2 Mbps scheme. CCK uses an eight chip code-spreading sequence and can operate in hostile radio environments with delay spreads of 100 ns at 11 Mbps, or 250 ns at the sub-rate speed of 5.5 Mbps. It can operate within the reduced band at 2.4 GHz

used in the Japanese market, allowing a single CCK baseband radio to be used worldwide [Ref. 20]. One of the main benefits of CCK, and the fundamental reason it was chosen, is its resistance to multi-path interference, which in turn allows these WLAN devices to provide better system performance. This 11 Mbps standard has given rise to faster transmit rates utilizing the high rate direct sequence spread spectrum (HR/DSSS) modulation technique. The multirate mechanism of the MAC layer warrants that the 11 Mbps operation can switch back to 5.5 Mbps if the radio channel is below the required value because of station separation distance or interference. Stations that are even further could switch back to the 2 Mbps or even the 1 Mbps capabilities of DSSS modulation. This thesis focuses on the testing of this technology by way of comparison with the 2 Mbps standard.

D. 802.11 Layer Reference Model

The 802.11 standard is limited in scope to the PHY and MAC network layers. The

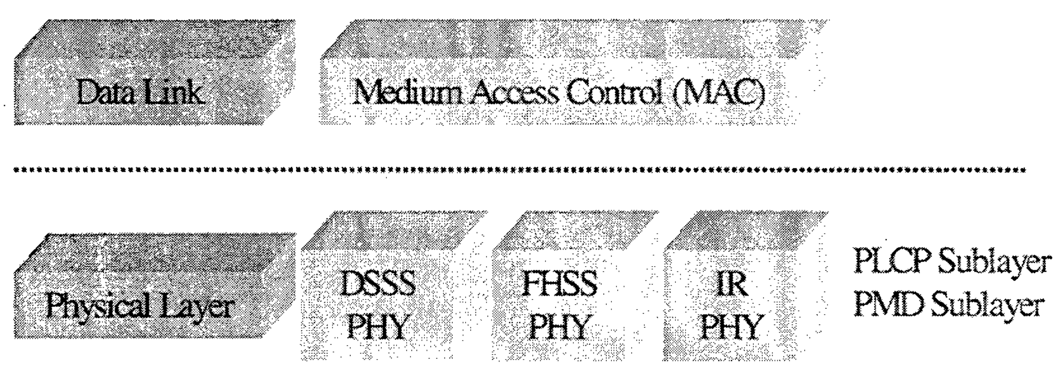


Figure 3.4: IEEE 802.11 Reference Model After Ref. [15]

IEEE 802.11 reference model is furnished in Fig. 3.4. The PHY directly corresponds to the lowest layer defined by the International Organization for Standardization (ISO) Open System Interconnect (OSI) 7-layer network model.

E. PHYSICAL LAYER

Up until now, IEEE 802.11 specifies five physical layers:

- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)
- Infrared (IR)
- High Rate Direct Sequence Spread Spectrum (HR/DSSS)
- Orthogonal Frequency Division Multiplexing (OFDM)

As discussed above, the last two are used in high speed WLANs. IEEE 802.11a uses OFDM and IEEE 802.11b uses HR/DSSS. The PHY is further divided into two sublayers, the Physical Layer Convergence Procedure (PLCP) sublayer and the Physical Media Dependent (PMD) sublayer.

1. Physical Layer Convergence Procedure Sublayer

PLCP sublayer defines a method of mapping the 802.11 PHY sublayer service data units (PSDU) into a framing format suitable for sending and receiving data between two or more stations using the associated physical medium dependent system. This allows the MAC layer to operate with minimum dependence on the PMD sublayer.

a) General PLCP Frame Format

The IEEE 802.11 PLCP frame format is illustrated in Fig. 3.5. The PLCP frame is composed of the Preamble, PLCP Header, MAC Data, and the cyclic redundancy check (CRC) fields.

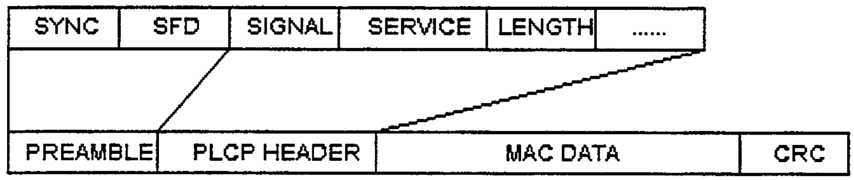


Figure 3.5: General PLCP Frame Format From Ref. [15]

The Preamble is PHY dependent. It includes two parts: Synchronization (SYNC) and the Start Frame Delimiter (SFD). SYNC is a sequence of scrambled ones and zeros, which is used by the PHY circuitry to select the appropriate antenna, and to reach steady-state demodulation and synchronization of the bit clock. The SFD is used to define frame timing. The PLCP is transmitted at 1 Mbps and contains logical information used by the PHY to decode the frame. The Signal field contains transmission rate information. The Service field is reserved for future use. The Length field indicates the MAC data length or the number of microseconds required to transmit the MAC data.

b) PLCP for FHSS

SYNC is an 80-bit field containing an alternating zero-one pattern, transmitted starting with zero and ending with one. The SFD consists of the 16-bit binary pattern 0000 1100 1011 1101, transmitted leftmost bit first. The first bit of the SFD follows the last bit of the sync pattern. The PSDU Length Word (PLW) specifies the number of octets contained in the PSDU. The 4-bit PLCP Signaling Field (PSF) defines the transmission rate ranging from 1 Mbps to 4.5 Mbps with 0.5 Mbps increments. The first bit of the PSF is reserved for future use. The FHSS PLCP frame format is shown in Fig. 3.6.

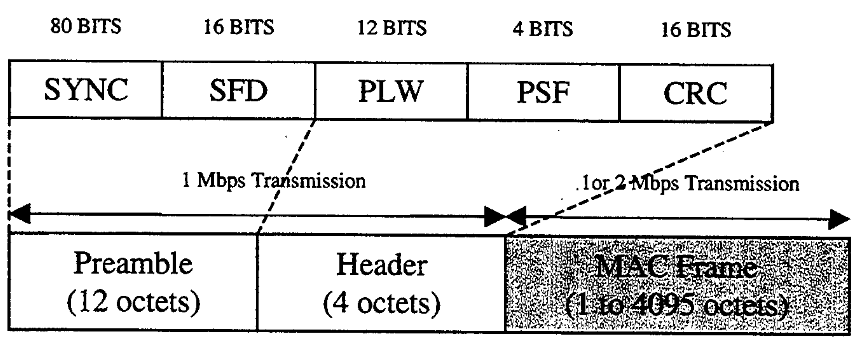


Figure 3.6: PLCP for FHSS After Ref. [15]

c) PLCP for DSSS and HR/DSSS

Figure 3.7 illustrates the DSSS and HR/DSSS PLCP frame format. The SYNC field is 128 bits. The SFD is a 16-bit 'hF3A0'. The SIGNAL field indicates the data rate:

1. 'h0A' for 1 Mbps
2. 'h14' for 2 Mbps

3. 'h37' for 5.5 Mbps

4. 'h6E' for 11 Mbps

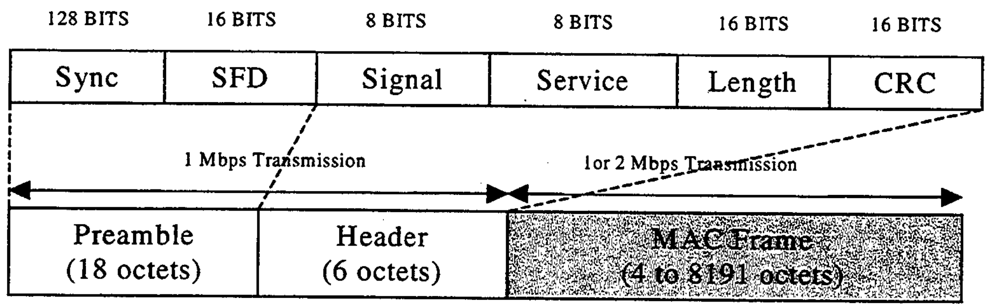


Figure 3.7: PLCP for DSSS and HR/DSSS From Ref. [15]

d) PLCP for OFDM

The PLCP preamble consists of 10 short and 2 long symbols. The SIGNAL field includes LENGTH, RATE and other fields. The RATE field conveys information about the type of modulation and the coding rate used in the rest of the packet. Table 3.2 shows valid RATE field options. The OFDM PLCP frame format is depicted in Fig. 3.8.

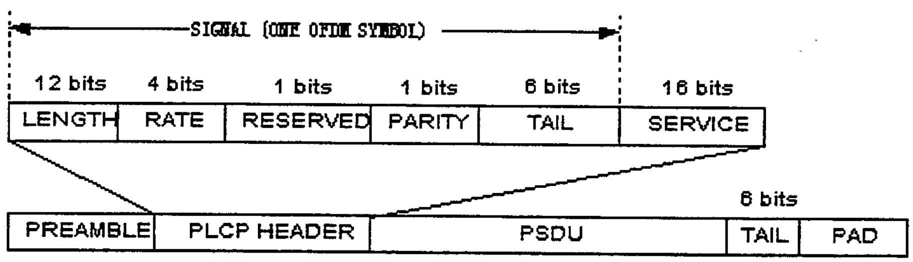


Figure 3.8: PLCP for OFDM From Ref. [15]

RATE	1011	1111	1010	1110	1001	1101	1000	1100
Data	6 Mbps	9 Mbps	12 Mbps	18 Mbps	24 Mbps	36 Mbps	48 Mbps	54 Mbps

Table 3.2: Rate Field Options After Ref. [15]

2. Physical Media Dependent Sublayer.

PMD sublayer defines the characteristics and method of transmitting and receiving data through a wireless medium between two or more stations each using the same modulation system.

F. MAC Layer

1. CSMA/CA with Acknowledgement

The IEEE 802.11 MAC layer was developed to work seamlessly with the standard Ethernet to ensure that wired and wireless nodes appear indistinguishable. If a station is ready to transmit, it first senses the medium, if the medium is busy, it will defer the transmission to a later time. Otherwise, it is allowed to use the medium. In the wireless world, the chance that a message sent from one station is not received by the destination station is much greater than in the wired world. To deal with this problem an acknowledgement (ACK) mechanism is utilized. The destination station will notify the sending station by way of an ACK when the message was successfully received. If the sender does not receive an ACK it can take the appropriate action and retransmit the message. [Ref. 15]

2. Hidden Station Problem

It is normal for a station to defer transmission when it senses another station is using the medium. In a wireless network the possibility exists that stations are hidden from each other. Because of the hidden node problem, collisions could occur. In figure 3.9, if both

station A and C try to send data to station B at the same time, a collision will occur. The collision avoidance scheme adopted in 802.11 requires a station to avoid transmitting while another node is actively transmitting.

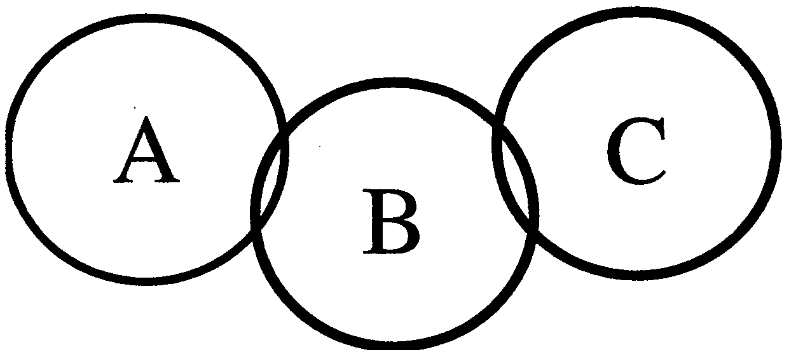


Figure 3.9: Hidden Node Problem After Ref. [19]

To avoid collisions, a Ready to Send/Clear to Send (RTS/CTS) mechanism is implemented. Figure 3.10 illustrates the basic concept of handshaking. When a station gets the chance to send, it sends a short RTS message, which contains the destination address

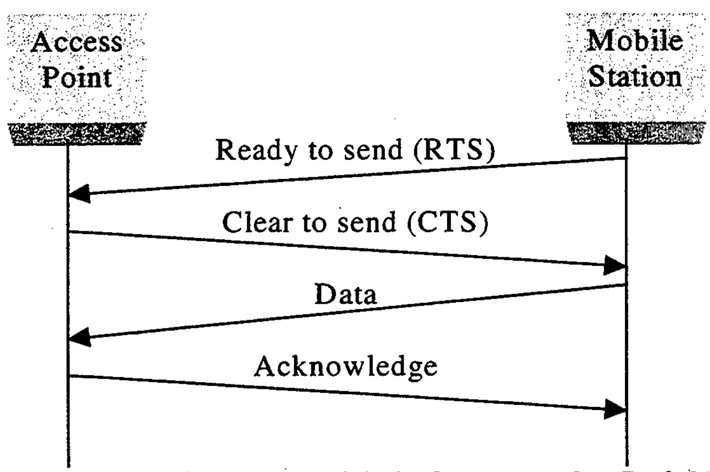


Figure 3.10: RTS/CTS Handshake Process After Ref. [19]

and the duration of the message. This RTS message informs other stations to back off for the duration. The destination station returns a CTS message if it is available to receive.

After the CTS signal is received, the source station can begin to transmit the data. Since the source station may not detect collisions, the destination will acknowledge every packet.

3. Topology

IEEE 802.11 specifies two different network topologies: ad-hoc and infrastructure. In the ad-hoc configuration, every station can communicate with any other station. There is no structure to the network. In the infrastructure configuration, there are some fixed points called Access Point (AP). A group of stations using the same radio frequency is called Basic Service Set (BSS). The mobile stations communicate through the AP.

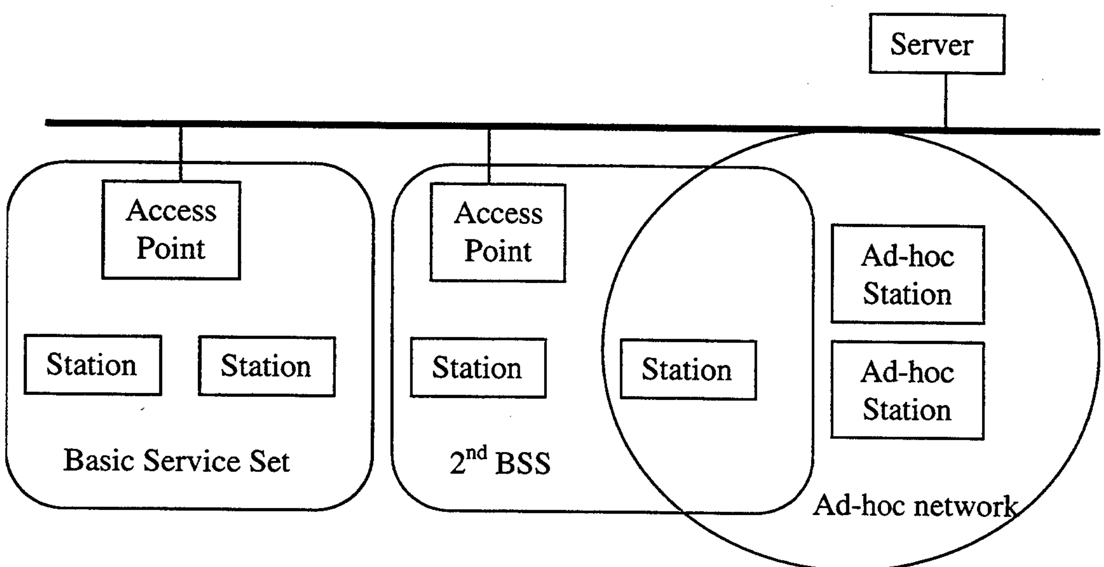


Figure 3.11: Infrastructure Configuration: Basic Service Set After Ref. [19]

4. Priority

The standard uses Inter Frame Spaces (IFS) to provide 4 types of priorities:

- SIFS - Short Inter Frame Space
- PIFS - Point Coordination Inter Frame Space

- DIFS - Distributed Inter Frame Space
- EIFS - Extended Inter Frame Space

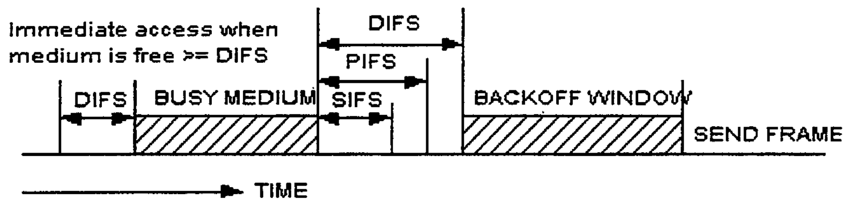


Figure 3.12: Priority through IFSs From Ref. [15]

The Inter Frame Spaces define a minimum time a station needs to wait after it senses the medium is free. The smaller the IFS, the higher the priority. If a collision occurs, an exponential back-off algorithm is used to compete for the medium.

5. Fragmentation

The MAC also supports a concept called fragmentation that provides for flexibility in transmitter/receiver design, and can be useful in environments with RF interference. An 802.11 compliant transmitter can optionally break messages into smaller fragments for sequential transmission. A receiver can more reliably receive the shorter date bursts because the shorter duration of each fragment transmission reduces the chance for errors due to signal fading or noise. Moreover, the smaller fragments have a better chance of escaping burst interference such as that from a microwave source.

The 802.11 standard mandates that all receivers support fragmentation but leaves such support optional on transmitters. Designers and end users can determine when or if fragmentation is used. For example, the designer could develop an adaptive scheme that dynamically enables fragmentation in the face of noise or interference. Designers could

also add the ability for the end user to enable fragmentation when transmission errors become a problem. Vendors can also use fragmentation as a price/performance trade-off. By assuming full-time fragmentation in a transmitter, the receiver can be designed with less expensive components resulting in lower receiver sensitivity. Fragmentation, however, incurs overhead on every fragment rather than every frame thereby reducing aggregate throughput of the network and the realizable peak throughput rate achieved between stations. [Ref. 18]

6. Roaming

The roaming provisions built into 802.11 also provide several advantages. For example, most existing WLANs require client nodes that roam from one AP to another all use the same channel. Typically the APs are connected by a wired backbone. When all of the APs use the same channel, the aggregate available throughput for the entire network is limited to the throughput on one channel. This limitation is quite necessary because offering 100% coverage in a cellular-like scheme requires that clients are sometimes within range of multiple APs.

The 802.11 standard includes mechanisms to allow a client to roam among multiple APs that can be operating on the same or separate channels. Each AP transmits a beacon signal every 100 msecs. The beacon includes a time stamp for client synchronization, a traffic indication map, an indication of supported data rates, and other parameters. Roaming clients use the beacon to gauge the strength of their existing connection to an AP. If the connection is judged weak, the roaming station can attempt to associate itself with a new

AP. The roaming station first performs a scanning function to locate a new AP on the same or different channel. The client can send probes to a number of APs and receive probe responses from each to judge the strongest AP. After finding the strongest signal, the client sends a reassociation request to the new AP. The AP must accept and acknowledge the request to complete the roaming procedure. The AP must also send an indication of the reassociation throughout the BSS LAN or distribution system. [Ref. 18]

7. Security

The IEEE 802.11 standard includes an encryption mechanism called wired equivalent privacy (WEP) that provides a security level equal to that of a wired network. The physical security of data transmission is gained by using spread spectrum technology, which makes it less vulnerable to interference. Data security using encryption is defined as an optional functionality of the MAC layer. WEP is only supplied between stations and not on an end-to-end basis. Furthermore, IEEE 802.11 does not specify any specific key management scheme to be used, hence, the task is left to the network operator. WEP only encrypts the data field of a frame while leaving headers unencrypted. This gives a potential eavesdropper the possibility to gather information about the usage of access points, and consequently, potentially useful information about network routines. [Ref. 21]

8. Power Saving

The IEEE committee recognized the fact that battery life is always an important factor when using a mobile system. The standard includes a power management scheme that allows a station to go into sleep mode in order to save power without losing the

network connection. The main idea behind power saving mechanisms is that the AP will maintain a list of stations currently working in power saving mode, and will buffer the packets sent to these stations. When the station requires a packet it must request it from the AP, this is done by sending a polling request, or by changing their mode of operation. The AP also periodically sends information about which power saving stations have packets buffered at the AP. The stations will wake up to receive beacon frames. If there are packets for them, they will stay awake and send a poll message to the AP to get the packets. [Ref. 15]

G. HIPERLAN

Although full-frame, broadcast quality video can be demonstrated at 4 Mbps, the WLAN bands only offer a limited capacity. The choice of radio depends largely on the application. For instance, FHSS is better suited to multiple-camera systems, whereas the superior multipath performance of DSSS is better suited for portable applications. In the future, increased demand could be met by the advent of the High Performance Radio LAN (HIPERLAN) standard. HIPERLAN is a European family of standards, developed by the European Telecommunications Standards Institute (ETSI), governing digital, high-speed, wireless communication in the 5.15-5.3GHz and the 17.1-17.3GHz spectrums. This standard addresses the need for higher bandwidth and improved protocols. Although the standard is primarily intended for office computing, support for MPEG video is expected. It boasts very impressive capabilities, including a data rate of 24 Mbps using a channel width of 23.5 MHz.

HIPERLAN was developed to achieve higher data rates than the initial IEEE 802.11 standard, which, specified data rates of 1 to 2 Mbps. An important feature of HIPERLAN is interoperability. The frequency bands allocated are 5.15-5.30 GHz for data rates of 24 Mbps and 17.1-17.3 GHz for data rates of 155 Mbps. No hub is required as the stations interact directly or through the nearest station available that can act as a bridging node. The full HIPERLAN data rate will be available at an approximate range of 50 m, but a limited 1 Mbps rate should be available up to 800 m. Rather than replacing the current variety of spread-spectrum radio systems, HIPERLAN will complement them where relatively short-range video transmission is required. HIPERLAN includes a family of four standards: HIPERLAN type 1, HIPERLAN type 2, HIPERACCESS (HIPERLAN type 3), and HIPERLINK (HIPERLAN type 4). The HIPERLAN family of standards is presented in Fig. 3.13.

Following the work done on the HIPERLAN/1 standard, ETSI is developing standards for Broadband Radio Access Networks (BRAN), which include the following systems:

- **HIPERLAN/2** – This short-range variant is intended for complementary access mechanism for Universal Mobile Telecommunications System (UMTS) systems as well as for private use as a WLAN type system. It will offer high-speed access (25 Mbps typical data rate) to a variety of networks including the UMTS core networks, ATM networks and IP based networks. Spectrum has been allocated in the 5 GHz range.
- HIPERACCESS – This long range variant is intended for point-to-multipoint, high-speed access (25 Mbps typical data rate) by residential and small business users to a

wide variety of networks including the UMTS core networks, ATM networks and IP based networks.

- HIPERLINK – This variant provides short-range, very high-speed interconnection of HIPERLANs and HIPERACCESS, e.g. up to 155 Mbps over distances up to 150 m. Spectrum for HIPERLINK is available in the 17 GHz range. [Ref .16]

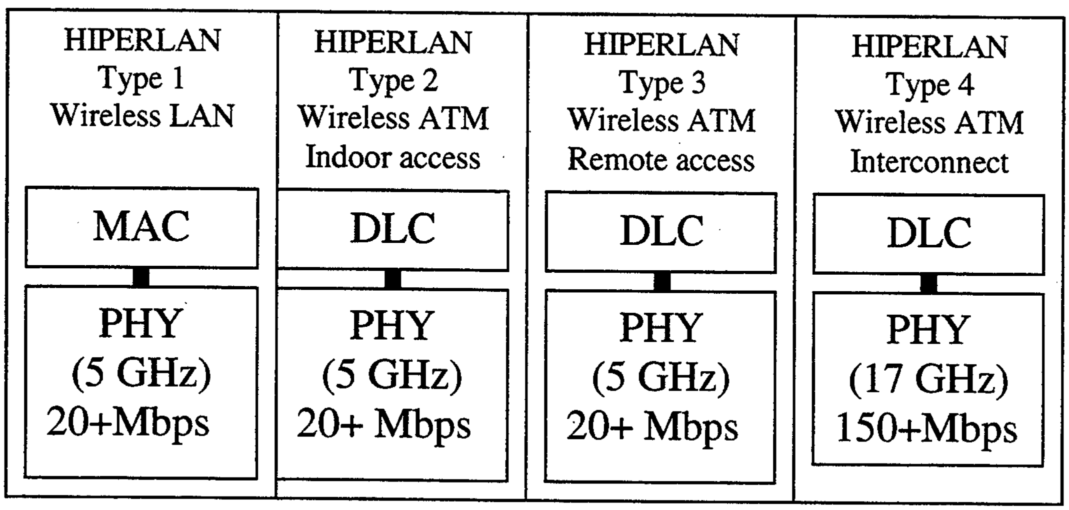


Figure 3.13: HIPERLAN Family of Standards After Ref. [22]

1. HIPERLAN/1 Reference Model

The focus of this discussion of HIPERLANs will be limited to the HIPERLAN/1 standard. HIPERLAN defines the operation of the lower portion of the Data Link Layer of the familiar OSI Reference Model and its 7-layer description of communication systems. The HIPERLAN/1 reference model is presented in Fig. 3.14. The Data Link Layer is usually subdivided into two parts when describing LANs – the Logical Link Control (LLC)

and Medium Access & Control (MAC) sub-layers. HIPERLAN only deals with the MAC sub-layer and its underlying PHY. [Ref. 23]

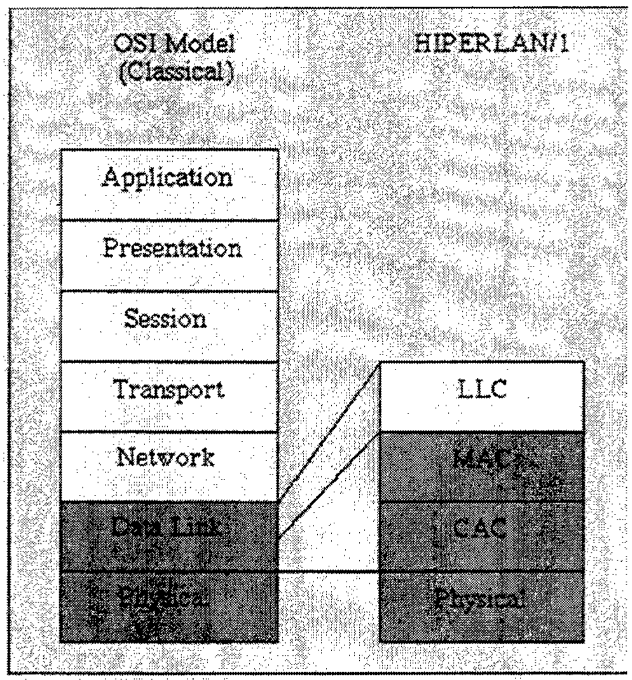


Figure 3.14: HIPERLAN/1 Reference Model From Ref. [23]

2. Physical Layer

The PHY dictates how the data transmission is handled between HIPERLAN devices. Three transmit power levels are defined, 50, 250 and 1000 mW, together with their corresponding receiver sensitivities.

a) RF carriers

HIPERLAN uses the radio frequency band 5.15-5.3 GHz. All transmissions must be centered on one of the nominal carrier frequencies, and all HIPERLAN equipment must operate on all 5 channels.

b) Clear Channel Assessment (CCA)

The HIPERLAN clear channel assessment scheme is based on the measurement of the received signal strength only. A threshold is used for determining whether the channel is busy or idle. Because the signal strength will vary with time, the time-domain variation of the received signal strength is used for threshold adaptation. The parameters for the measurement of signal strength is expressed as Signal Level Number (SLN). Because HIPERLAN signals are bursty in nature and any interference will be of relatively constant power level, the channel shall be considered to be idle when the received SLN is less than the threshold value. In all other cases the channel is considered busy. When the channel is busy, the threshold adaptation algorithm seeks to raise the threshold to just above the level of any continuous signal on the channel. [Ref. 15]

c) Modulation

Gaussian Minimum Shift Keying (GMSK) is used as the high bit rate modulation scheme. The PHY specification defines a GMSK modulation scheme and 3 or 5 channels in 100 or 150 MHz depending on national allocation. GMSK is a constant envelope modulation scheme, which means that the amplitude of the transmitted signal is constant. HIPERLAN encodes a single digit of information for each pulse transmitted (1 bit/Hz) and hence, in order to reach the very high data rate of greater then 20 Mbps, the pulses are very short, approximately 42 nanoseconds. Such short pulses suffer from what is known as Inter-Symbol Interference, which means the receiver has to extract the transmitted signal from the received signal, where different pulses have been spread out and overlap

each other [Ref. 23]. FSK is used as the low bit rate modulation scheme to modulate a low rate transmission.

3. Channel Access and Control (CAC) sub-layer

An intermediate layer, the Channel Access and Control (CAC) sub-layer, is introduced in the HIPERLAN/1 architecture to deal with the channel access signaling and protocol operation required to support packet priority. The CAC layer defines how a given channel will attempt access depending on whether the channel is busy or idle, if contention is necessary, and at what priority level the attempt will be made. The CAC layer implements a pseudo-hierarchically independent access mechanism to achieved active signaling in a listen-before-talk access protocol. This mechanism, Elimination-Yield Non-Preemptive Multiple Access (EY-NPMA), codes priority level selection and contention resolution into a single, variable length radio pulse preceding packet data. EY-NPMA provides good residual collision rate performance for even large numbers of simultaneous channel contenders.

A transmission passes through three phases: the prioritization phase, the contention phase and the transmission phase. The transmission phase forms the channel free channel access cycle because during the transmission the medium is considered free. The whole three phases forms a synchronized channel access cycle. CAC works in the following three steps:

1. During the prioritization phase, the data transmissions with highest channel access priorities are selected out. Channel access priority is based on packet residual lifetime and user priority.
2. In the contention phase, CAC competes with any other HIPERLAN CAC with the same priority. CAC transmits a signal, at the end of transmission the CAC listens to the channel. If another device is still transmitting, it defers its transmission until the next channel access cycle. Otherwise the CAC gains the channel and begins its transmission.
3. Data is transmitted in the transmission phase.

Due to the non-preemptive requirement, a data transmission can compete for the channel only if it's ready at the beginning of a channel access cycle. The channel access and control cycle is outlined in Fig. 3.15.

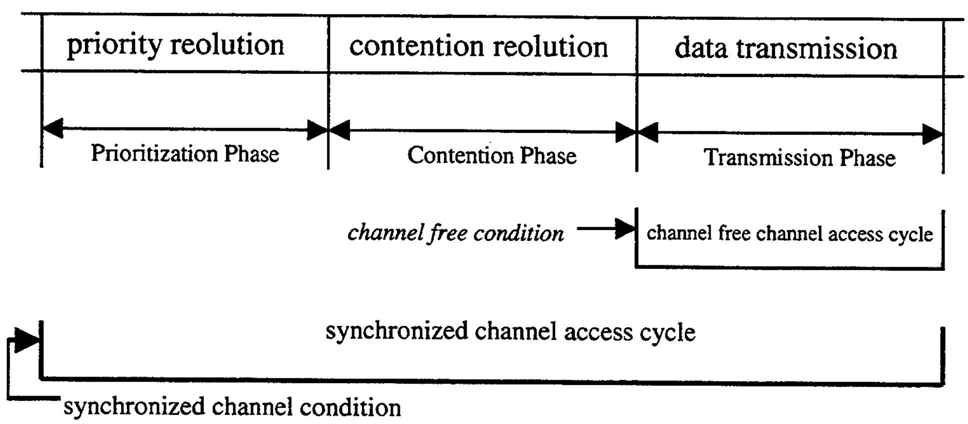


Figure 3.15 Channel Access and Control After Ref. [23]

4. MAC sub-layer

The HIPERLAN/1 architecture includes a sophisticated MAC sub-layer structure to hide the inherently unreliable nature of the radio medium from the MAC client layers. The HIPERLAN/1 standard does not specify a LLC layer. Acknowledged unicast transmissions and unacknowledged multicast transmissions are supported by the HIPERLAN/1 MAC service. The acknowledged transmission may be re-tried any number of times within the lifetime of the request. Once the lifetime interval has expired the associated data is discarded and resources re-allocated to other HIPERLAN/1 layer functions. The MAC layer defines the various protocols that provide the HIPERLAN features of power conservation, security, and multi-hop routing, as well as the data transfer service to the upper layers of the protocol.

a) Topology

HIPERLAN/1 is designed to work without any infrastructure but supports both infrastructure and ad-hoc topology. In the infrastructure topology, each HIPERLAN device will select one and only one neighbor as Forwarder and transmits all traffic to the Forwarder. In ad-hoc topology, there is no such controller; every device can communicate directly with each other. The simplest HIPERLAN thus consists of two stations. The two stations may exchange data directly, without any interaction from a wired (or radio-based) infrastructure. Further, if two HIPERLAN stations are not in radio contact with each other, they may use a third station (i.e. the third station must relay messages between the two communicating stations). [Ref. 15]

b) Priority

In IEEE 802.11, priority is embedded in the Inter-Frame Spacing mechanism, thus the priority is fixed. HIPERLAN assigns channel access priorities dynamically to the packets. As mentioned above, HIPERLAN uses the following two parameters to calculate the priority:

- packet lifetime
- user priority

Since packet lifetime is updated constantly, the priority will increase with time. When it's getting near to the packet expiration, its priority will increase to the highest point.

c) Multi-Hop Routing

HIPERLAN uses "Hello" messages to do neighborhood discovery. Each device will periodically send a "Hello" packet to its neighbors. One type of "Hello" packet will carry a list of the sender's neighbors. Forwarders use this information to construct a fully connected map of the extended HIPERLAN. Then it can decide which device will be the next hop for a given destination and it can forward packets from one hop to another.

d) Security

The HIPERLAN security architecture is very similar to the method defined in the 802.11 specification. The Wire Equivalent Privacy (WEP) algorithm was proposed to the HIPERLAN committee, which accepted the principle. However, the implementation in HIPERLAN is different.

Each HIPERLAN packet carries a two-bit field in the payload header that tells whether the payload is encrypted or not. If it is, the header identifies one of three possible keys. Since the actual key is an implementation choice, as is the interpretation of the key identifier, any arbitrary key distribution scheme may be used.

The Key Identifier field in the HIPERLAN packet header can be implemented in different ways to provide varying degrees of security. To protect against casual eavesdropping or data insertion, a constant key can be used to encrypt the data. The advantage of this simple protection is that it needs little management, but it is more susceptible to well known attacks. By adding a key management system, any degree of protection, up to and including the unbreakable 'one-time-pad' can be constructed. [Ref. 23]

e) Power Saving

By way of comparison, the HIPERLAN power conservation mechanism is quite different to that employed in 802.11, where the power conservation mechanism is tied to the operation of the AP. In HIPERLAN, mobile devices can agree upon awake patterns (e.g., periodic wake-ups to receive data). Some nodes in the networks must be able to buffer data for sleeping devices and to forward the data at the right time. The power conservation functions are performed by two roles: p-supporter and p-saver. P-saver is the power-conserving device, and p-supporter is the neighbor of p-saver who defers transmission of packets to the p-saver. P-saver will broadcast to its neighbors the pattern of when it will sleep and when it will wake. Using such information, p-supporter can know when to transmit the buffered packets to p-saver. In this mechanism, the periodicity and

length of the sleep/wake intervals can be selected to match different application needs, and hence obtain maximum benefit from the power conserved. [Ref. 23]

H. PRODUCTS

1. WaveLAN IEEE Turbo 11Mb PC Card

- Compliant with the IEEE802.11b High Rate (HR) wireless standard
- 2.4 GHz Direct sequence spread spectrum (DSSS)
- 4 speed options (11 Mbps, 5.5 Mbps, 2 Mbps and 1 Mbps)
- Built-in security features
- Interoperable with other high-speed 802.11b compliant systems

2. Aironet Wireless LAN products

- IEEE 802.11 compliant
- 2.4 GHz Direct sequence spread spectrum (DSSS)
- 4 speed options (11 Mbps, 5.5 Mbps, 2 Mbps and 1 Mbps)

The following chapter presents a more detailed view of several wireless technology options. The chapter includes a discussion on the comparison between DSSS and FHSS modulation and how each deal with interference suppression. The concept of correlation is introduced followed by an explanation of complementary code keying (CCK), which enabled the jump in data rate from 2 Mbps to 11 Mbps.

IV. WIRELESS TECHNOLOGY OPTIONS

A. NARROWBAND TECHNOLOGY

A narrowband radio system transmits and receives information on a specific radio frequency, concentrating power at an assigned center frequency. Narrowband radio keeps the RF signal as narrow as possible to pass the information without interfering with the surrounding spectrum users. Crosstalk between channels is avoided by carefully coordinating different users on different channel frequencies.

A private telephone line is much like a radio frequency. When each home in a neighborhood has its own private telephone line, people in one home cannot listen to calls made to other homes. Privacy and noninterference are accomplished by the use of separate radio frequencies [Ref. 24]. All unwanted signals can be filtered out with the use of a specially designed filter, that passes only the desired signals at a designated frequency.

B. SPREAD SPECTRUM COMMUNICATIONS

Spread spectrum technology is simply another RF modulation technique designed to minimize the average power at any given frequency over time, gaining reliability by increasing redundancy. This is accomplished by "spreading" the signal over the entire available band, and requiring the receiver to know where to look for the pieces of the signal. This redundancy has the additional benefit of minimizing the effects of interfering walls and structures. [Ref. 25]

By spreading the data transmission over a large bandwidth, the average power level at any one frequency is reduced, causing less interference to other frequencies in the band. If implemented appropriately, the other frequencies will also interfere less with your signal, even if they do not employ spread spectrum techniques. [Ref. 24]

Claude Shannon produced a groundbreaking paper on the mathematical theory of communication in 1949. Shannon's resulting theorem can be expressed as:

$$C = BW \log_2 [51 + SNR] \text{ bits per second} \quad [4.1]$$

Where: C = data rate in bits per second

BW = bandwidth (Hz)

SNR = average signal power (W)/mean white Gaussian noise power (W)

It can be seen from the equation that the only options available to increase a channel's capacity are to increase either the BW or the SNR. An increase in the SNR requires an increase in transmitter power as the noise within the channel is beyond our control. Thus we can either trade power or bandwidth to achieve a specified channel data rate. Because of the logarithmic relationship, increasing the power output is often unrealistic. However if frequency allocation constraints permit, the bandwidth can be increased. An appreciable increase in data capacity or SNR (for a fixed data rate) can then be achieved.

Spread spectrum systems utilize very wide bandwidths and low SNRs. From Shannon's theorem and a little algebra, we get:

$$C/BW = 1.44 \text{ Log}_e [1 + SNR] \quad [4.2]$$

In a spread spectrum system the SNR is typically small, much less than 0.1, we get:

$$C/BW = 1.44 \text{ SNR} \quad [4.3]$$

From the derived relationship it can be clearly seen that a desired SNR for a fixed data rate C, can be achieved by increasing the transmission bandwidth [Ref. 26]. This is represented in Fig 4.1 where $BW_{RF} >> BW_{INFO}$.

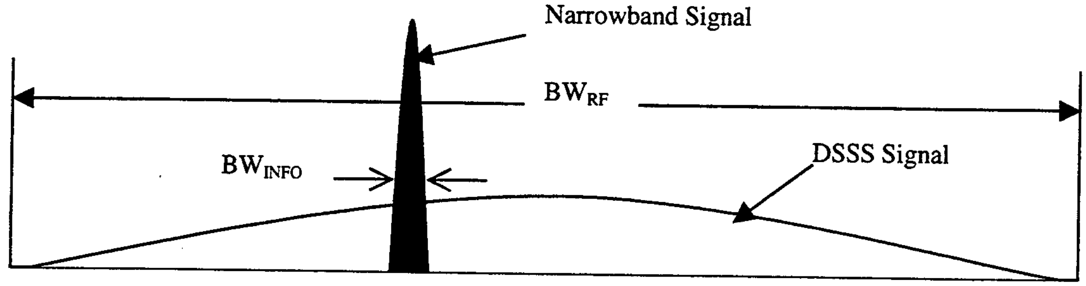


Figure 4.1: Spread Spectrum vs. Narrowband Transmission After Ref. [27]

Communications signals can be greatly increased in bandwidth by combining them with binary sequences using several techniques. The result of this spreading has two beneficial effects. The first effect is dilution of the signal energy so that while occupying a very large bandwidth, the amount of power density present at any point within the spread signal is very low. Spectral power density is the amount of watts of RF power present per Hz of bandwidth. By nature of the spreading process, the output power of the spectrum transmitter is typically spread over many MHz of bandwidth. Thus for a direct sequence transmitter of 1 W output and a spread bandwidth of 8 MHz the power spectral density is:

$$1 \text{ W} / 8{,}000{,}000 \text{ Hz} = 125 \text{ nW} / \text{Hz} \text{ [Ref. 26]} \qquad [4.4]$$

The amount of signal dilution depends on several factors such as transmitter power, distance from the transmitter and the width of the spread signal. The dilution may result in the signal being below the noise floor of a conventional receiver, and thus invisible to it, while it can clearly be received with a spread spectrum receiver.

The second beneficial effect of the signal spreading process is that the receiver can reject strong undesired signals, even those much stronger than the desired spread spectrum signal power density. This is because the desired receiver has a copy of the spreading sequence and uses it to "de-spread" the signal. Non-spread signals are then suppressed in the despreading or correlation process. The effectiveness of spread spectrum's interference-rejection property has made it a popular military anti-jamming technique.

Stored reference (SR) systems make use of a predetermined spreading signal known to both the transmitter and the receiver. The spreading signal cannot in this case be truly random for obvious reasons. SR systems make use of codes that are pseudo-random in nature. In general, pseudo-random noise (PN) codes have the following properties:

- In each period of the sequence, the number of ones differs from the number of zeros by no more than one.
- The length of a run of consecutive bits of one type (i.e. all zeros or all ones) should vary such that about half of the runs are one bit in length, one quarter of the runs are two bits in length, one eighth of the runs are three bits in length and so on.
- The correlation of the spreading code with a shifted version of itself should be a maximum when the two sequences are aligned and a minimum for all other positions.

For recovery of the information signal in a SR system, it is absolutely essential that the receiver's code sequence be synchronized with the transmitter's sequence. In addition, the desired signal properties and multiple access requirements will dictate the nature of the PN codes that will be employed by a spread spectrum system. [Ref. 27]

Signals not bearing the desired pseudo-random or linear recursive coding sequence are rejected. The result is a type of private channel, one in which only the spread spectrum signal using the same PN sequence will be accepted by the spread spectrum receiver [Ref. 19]. By using different pseudo random codes, several independent communications links may simultaneously operate in the same frequency range. Moreover, the same multiplying action that correlates with the desired signal further spreads any interfering signals. [Ref. 28]

All spread spectrum applications start with a desired channel data rate that can be carried over a normal RF carrier assigned to a fixed channel frequency. In a licensed application, which has exclusive use of that channel with the guarantee of no interference, spread spectrum still offers frequency reuse, as well as a measure of security. Unfortunately, there is not enough available frequency spectrum to allow unique channels for all applications. As a result, certain bands of frequencies have been allocated for shared use on an unlicensed basis. It is in these bands that spread spectrum techniques make reliable communications possible. [Ref. 28]

A key characteristic of a spread spectrum signal is process gain. Process gain can be approximated by the ratio between the PN code bits and the symbol rate of the desired data.

$$G_p = \text{chip symbols/data symbol} \quad [4.5]$$

For example, a system that spreads each symbol by 256 chips per symbol has a ratio of 256 to one. This value is determined by the expression (generally expressed in dB):

$$G_p\,(\text{dB}) = 10 \log_{10} (\text{chips/symbol}) \quad [4.6]$$

or 24dB for 256 chips per symbol [Ref. 28]. The process gain indicates the gain improvement exhibited by a spread spectrum system by nature of the spreading and despreading process. It is a measure of the ability of the system to overcome interference. [Ref. 24]

C. SIGNAL SPREADING

The channel data may be either analog or digital, but for simplicity, we will consider a basic digital data system. There are three popular means for spreading the data signal. The first two are variations of frequency hopping (fast and slow), and the last technique is direct sequence spreading. Figure 4.2 is provided to serve as an example of a representative frequency hopping pattern.

1. Frequency Hopping (Slow Hoppers)

In this technique, the data signal is transmitted as a narrow band signal wide enough to carry only the required data rate. At specific intervals (the hop rate), this narrow band

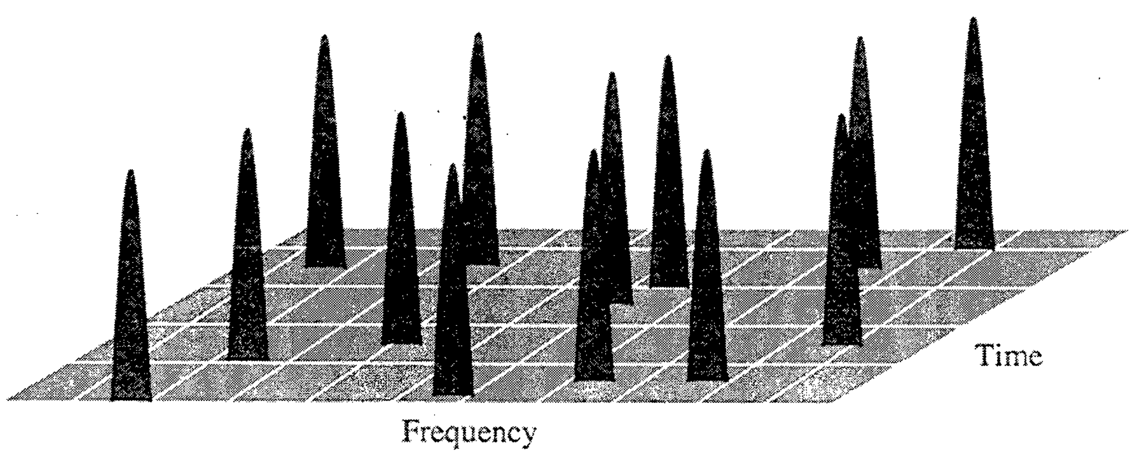


Figure 4.2: Spectrum of a Frequency Hopper After Ref. [27]

signal is moved, or hopped, to a different frequency within the allowed band. The amount of time the signal is present in any channel is called the dwell time.

The sequence of frequencies follows a pseudo random sequence known to both the transmitting node and the receiving node. Once the receiving node has acquired the hopping sequence from the transmitter, one or more data packets are transmitted before the frequency is hopped to the next channel. The basic characteristic of a slow hopper is that many data bits are transmitted between hops. This approach is readily understandable and relatively low cost to implement. It offers the advantage of being able to recover data lost during one transmit cycle by retransmitting the same data on another channel that is less impacted by interference. However, these systems may dwell on one frequency for an extended period of time, which risks the loss of a considerable amount of data and will require correction.

Slow frequency hoppers are best characterized as frequency-agile, narrow-band data radios. At each specific frequency, they have essentially the same performance and interference susceptibility as any narrow band radio. Their performance is actually less than a narrow band radio due to the time lost during the periodic frequency changes. [Ref. 28]

2. Frequency Hopping (Fast Hoppers)

Fast frequency hoppers work in a similar manner as slow hoppers, except that the hop rate is significantly faster. Fast hoppers make many hops for each bit of data that is transmitted. Under this technique, each data bit is transmitted multiply on several different frequencies. At the receiving end, the receiver needs only to receive the majority of the

redundant bits correctly to recover the data without error. The real benefit of the fast hopper is that true process gain is provided by the system because of this redundancy of the data transmission. Even if interference in the band blocked out one or more narrow band channels, the data would not be lost.

Implementation of the fast frequency hopping approach, however, is complex and expensive because of the problems in making rapid frequency shifts while maintaining frequency and phase coherency in the data channel. As a result, most fast hoppers operate with relatively low data rates. [Ref. 28]

3. Direct Sequence Spread Spectrum

Direct sequence spread spectrum grew from a need to increase performance and reduce cost of fast hoppers. The basic problem was to increase the hopping rate so that either each data bit could be more redundantly encoded (more process gain), or that a higher bit rate could be transmitted, even though data rate and process gain are inversely proportional. The solution came in realizing that a PN digital code contains all the frequencies from DC to the code clock rate, illustrated in Fig 4.3. [Ref. 28]

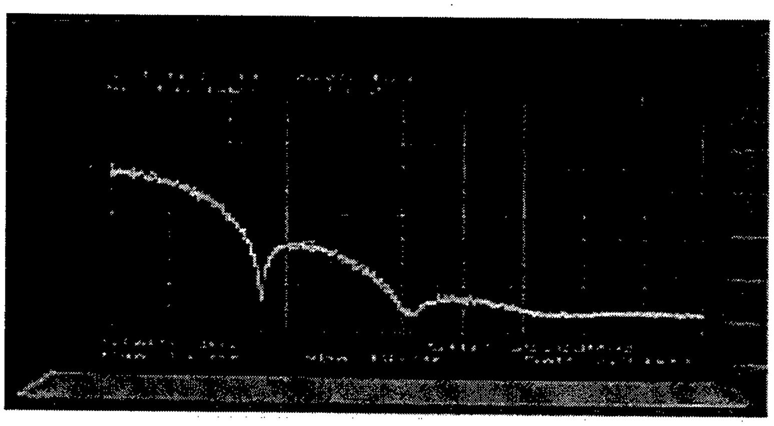


Figure 4.3: Pseudo-Random Digital Code From Ref. [28]

DSSS generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chipping code. The longer the chip, the greater the probability that the original data can be recovered and, of course, the more bandwidth required. As evidenced by Fig. 4.4, when the narrow band data signal and the pseudo random code sequence is multiplied, the signal spectrum is spread to a bandwidth twice that of the code. [Ref. 28]

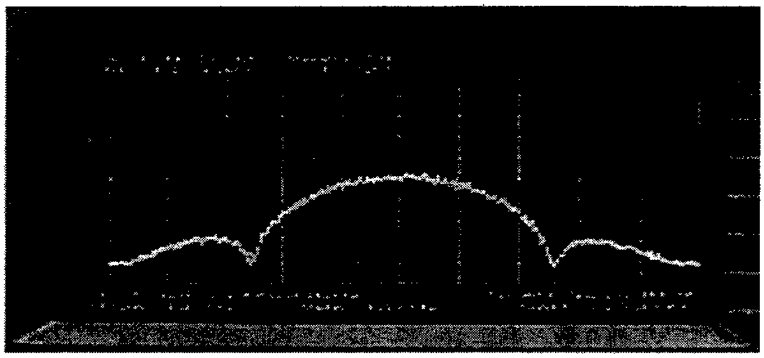


Figure 4.4: Doubled Bandwidth From Ref. [28]

Figure 4.5 shows that by multiplying the pseudo noise spread signal with a copy of the same pseudo noise, the original data signal is recovered.

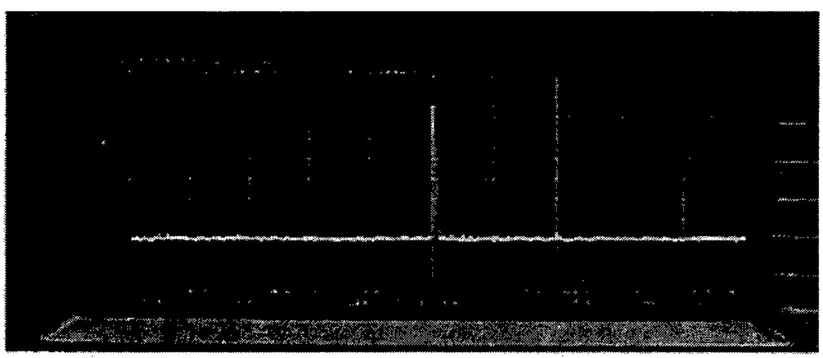


Figure 4.5: Recovered Original Data Signal From Ref. [28]

Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for

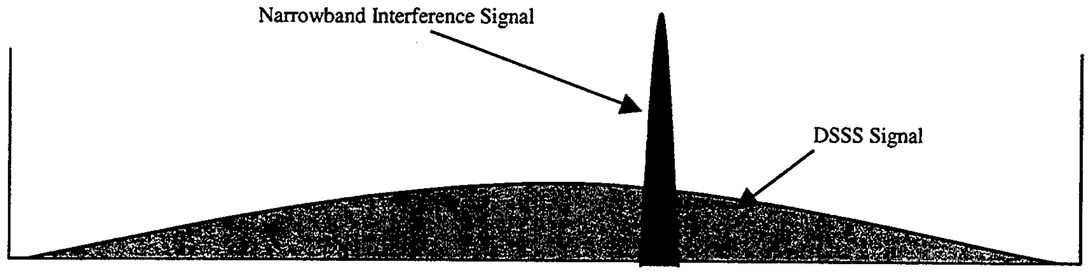
retransmission. To an unintended receiver, DSSS appears as low-power wideband noise and is rejected by most narrowband receivers [Ref. 24]. Correlation only occurs if the codes are identical and perfectly aligned within a fraction of the code clock.

D. INTERFERENCE SUPPRESSION

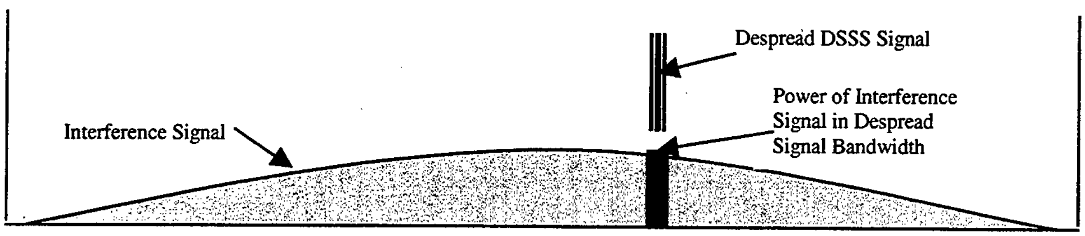
One important reason for using spread spectrum techniques is to reduce the effects of interference on a communications link and in turn reduce the likelihood of the signal being jammed intentionally. By using a wider bandwidth than necessary for signal transmission, a signal can still be recoverable even with a very low SNR. As mentioned above, this is due to the fact that there is a processing gain associated with spread spectrum signals and that processing gain is proportional to the amount that the signal is spread. Most spread spectrum systems have a processing gain of at least 10. A spread spectrum receiver with a large processing gain can actually function with SNRs of less than unity i.e. the noise power at the receiver is greater than the received signal. Although both direct sequence and frequency hopping systems have an associated processing gain, the mechanism that suppresses interference is different for each technique. [Ref. 27]

1. Resistance to Narrowband Interference

Figure 4.6 illustrates the effects of a narrowband interference on a direct sequence signal. Because the correlation process at the receiver is essentially a spreading process (the received signal is modulated with the spreading code), the receivers despreading process will spread a narrowband interference. The result is that the power of the interference is



Before Signal Despread



After Signal Despread

Figure 4.6: The Effect of Narrowband Interference on a DSSS Signal After Ref. [27]

spread out over a large bandwidth and only a small amount will affect the despread information signal.

In the case of frequency hopping, a narrowband interference may wipe out one hop of the sequence but the other hopping channels will remain unaffected, as illustrated in Fig 4.7. An intelligent frequency hopper can avoid hopping to channels where there is interference and thus may only be effected once. [Ref. 27]

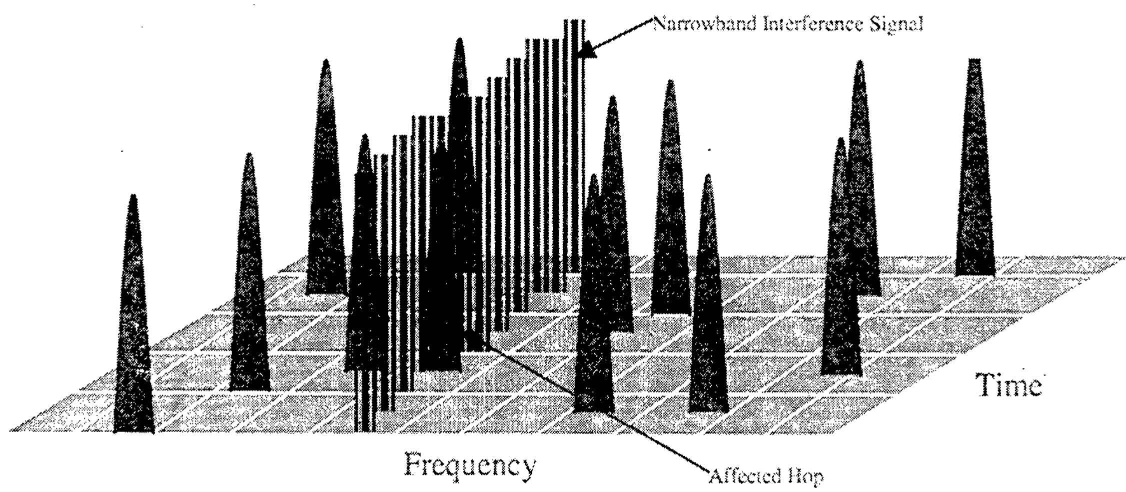


Figure 4.7: The Effects of a Narrowband Interference on a FHSS System After Ref. [27]

2. Resistance to Multipath Fading

One particularly detrimental form of interference is caused by multiple reflections of a transmitted signal reaching the desired receiver. This phenomenon, known as multipath can result in signal nulls and errors due to delay spread. Such multiple paths may be due to reflections from stationary or non-stationary objects as well as atmospheric reflection or refraction. In general, multipath becomes much worse as the frequency of operation and data rate increase. Most broadband wireless (>2Mbps) transmission systems require some form of anti-multipath measures. Mobile systems are particularly susceptible to multipath as receivers can move in and out of fades.

As previously mentioned, spread spectrum systems are inherently resistant to multipath. In the case of direct sequence systems, the code-correlation receiver effectively ignores reflected signals. Frequency hoppers can get around multipath by hopping faster than the fade rate, thus avoiding signal nulls.

E. CORRELATION

Correlation is a fundamental process in a spread spectrum system. Correlation measures how similar two signals are in appearance to each other. In a spread spectrum receiver, correlation is often used to identify a signal that has been coded with a desired PN sequence. Correlation is usually done with a circuit known as a correlator. A correlator is typically composed of a mixer followed by a low-pass filter that performs averaging. The mixer multiplies the two signals to be compared. A match yields a high value of output; but if the two mixed signals differ, the output will be lower depending on how different the signals are. The averaging circuit reports the average output of the mixer or the average likeness of the two signals.

1. DSSS Correlation

In a DSSS system, the correlator is used to detect and identify signals with the desired spreading code. Signals spread with other PN codes, or signals not spread at all, will differ statistically from the desired signal and give a lower output from the correlator. The desired signal will have a strong match with the locally generated PN code and yield a larger output from the correlator.

Notice that the averaging circuit of the correlator gives the average mixer value over time. If noise or interference is present, some of the received signal will be corrupted. After mixing, the interfering signals are spread and resemble noise, while the desired signal is despread and narrow band. The averaging circuit then performs a low-pass filter function, thereby reducing the noise while passing the desired narrow band information.

This low-pass filter function is the heart of the direct sequence interference-rejection process. [Ref. 25]

2. FHSS Correlation

Correlation in a FHSS system is implemented differently but the concept is the same. In a frequency hopping system, the transmitter carrier frequency is being moved many times a second according to the spreading sequence. The receiver uses the same spreading sequence to follow the transmitter, moving from channel to channel in exact step with the signal. If the receiver is out of step with the signal, it cannot recover the information being transmitted. FHSS signals that are under the control of a different PN sequence will be received only randomly, by the chance that both the desired and undesired PN codes have a channel in common at that moment. [Ref 25]

F. CIRCUIT OPERATIONS

The circuit in Fig 4.8 is very similar to circuits used in other types of RF communications applications, such as the U.S. digital cellular standard IS54 and Low Earth Orbit (LEO) satellite terminals. The signal chain block shows both a receive channel and a transmit channel. The receiver signal chain works in several stages: it takes a lower frequency channel sitting on a high frequency carrier signal down in frequency to baseband, where it is digitized and processed by the DSP and then directed to the computer. The carrier frequency is usually at 2.4 GHz or 5.8 GHz, depending upon the application. The received signal at the antenna is initially very weak. This signal is then filtered and amplified by a specialized low-noise amplifier (LNA). The filtered signal is then fed into a

mixer, which performs a frequency down-conversion to a lower frequency, often referred to as the IF or intermediate frequency. The synthesizer provides a suitable mix-down frequency, for the mixer. This intermediate frequency can be variable depending upon the specific application.

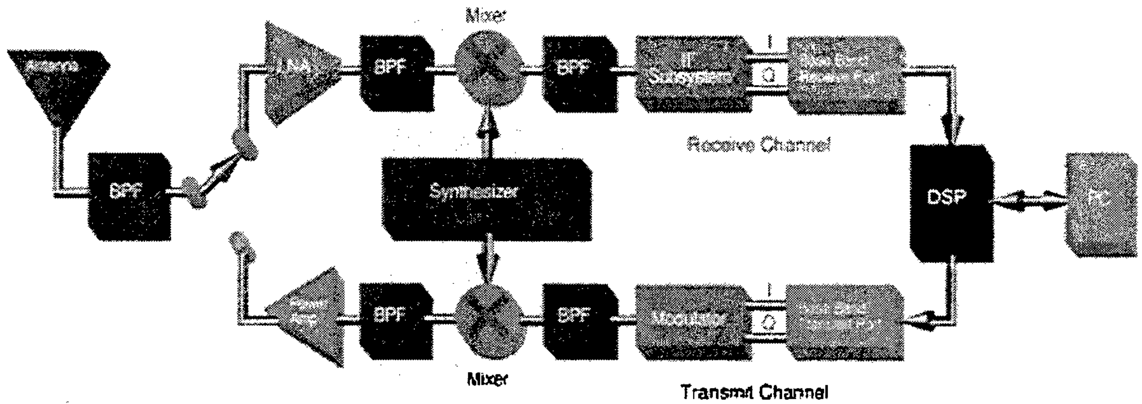


Figure 4.8: Typical RF Transmitter/Receiver Circuit From Ref. [24]

Next, the mixed-down signal is fed into the IF subsystem, where it is amplified and demodulated. The IF subsystem provides two quadrature signals which are sampled 90 degrees apart. These signals are called the in-phase (I) and quadrature (Q) signals. These quadrate signals are then digitized and filtered by the baseband receive port and then fed into the DSP. The DSP performs complex functions like echo cancellation and signal processing, then formats the data into a suitable format for the PC or computer terminal. The transmit channel essentially performs all of these functions in reverse. The digital data from the PC is coded and modulated, then frequency shifted up to the carrier frequency by the mixer. The signal is then amplified by the power amplifier and then transmitted out via the antenna. [Ref. 24]

G. COMPLEMENTARY CODE KEYING

Task Group B (802.11b), designed to deliver Ethernet speeds, uses a complementary-code-keying (CCK) waveform, jointly developed by Harris and Lucent Technologies. CCK delivers on four goals the committee deemed critical, concerning speed, interoperability, bandwidth usage and worldwide compatibility. Addressing the speed issue, CCK delivers very robust Ethernet-equivalent data rates of better than 10 Mbs. Interoperability is enhanced because this approach allows downshifting that makes it interoperable with existing 1 and 2 Mbs 802.11 networks. CCK operates within the existing DSSS 1 and 2 Mbs channels of the 2.4 GHz ISM band. And, like the 1 and 2 Mbs standard, this extension is truly compatible with worldwide standards developed by global regulatory bodies such as the Federal Communications Commission, the European Telecommunications Standards Institute, and the (Japanese) Radio Equipment Inspection and Certifications Institute (MKK).

In addition to meeting those critical goals, CCK provides another important characteristic, a strong immunity to multipath interference. CCK is extremely resistant to echoes and, because of its exceptional delay spread specifications, 100 nanoseconds at 11 Mbps and 250 nanoseconds at 5.5 Mbps, it can work in a variety of hostile RF environments. CCK's eight-chip complementary code spreading sequence also enables it to achieve high transmission speeds without compromising security or robustness.

CCK is a form of M-ary orthogonal keying (MOK) modulation where the code symbols are four phase modulated. Since CCK's symbols are QPSK in nature, they

simultaneously occupy both the I and Q channels. The code set of complementary codes is very rich. Thus, by using a set of 64 codes, CCK-based WLANs can modulate 6 bits on the M index and 2 bits on QPSK to create an 8 bit code symbol that, in effect, has 16 bits of complexity. One of the main benefits of CCK is its ability to handle multipath interference. In multipath conditions, the absence of simultaneous orthogonal signals in CCK minimizes cross rail interference. This allows CCK-based devices to be less susceptible to multipath interference, which in turn allows these WLAN devices to provide better system performance. [Ref. 29]

THIS PAGE INTENTIONALLY LEFT BLANK

V. COMPONENT TESTING

The purpose of this chapter is to present the results of the test conducted on various wireless IEEE 802.11b compliant components. The objective of this test was to comparatively assess the performance of two commercially available components, meeting the provisions specified in the IEEE standard for higher speed wireless networks. To ensure consistency, a representative component was chosen from the components evaluated in the thesis by Matthews [Ref. 4]. This component, previously evaluated, provided a common link in the testing conducted between IEEE 802.11 and IEEE 802.11b compliant components.

The results presented here are based on testing conducted on campus at the Naval Postgraduate School (NPS) in Monterey, California. It is the goal of this thesis to present the performance characteristics of the latest components available in the wireless technology field and to establish a basis for continued research in the area of wireless local area networks for deployment onboard U.S. Naval vessels.

Testing was executed in two phases, both of which were conducted outdoors. Outdoor testing was necessary in order to compile data transfer rate results from ranges in excess of 500 feet. The first phase of testing was conducted line-of-sight (LOS), where the wireless PCMCIA adapter card had a direct path propagation component to a wired access point. The second phase was a non-line-of-sight (NLOS) assessment, where there was no direct path propagation component and communications were only possible via reflected signals. Of course, the results presented here are not meant to be indicative of the

performance that would be achieved onboard a ship. The materials, construction and compartmentalization present onboard a naval vessel would confer a much harsher environment than the one provided here. This test is to mainly provide a comparison of the components presently available in order to provide a gauge as to which of these components may possibly operate the best onboard a ship and best suit the needs of the Navy.

Since the purpose of this test was to stringently focused on the performance of the wireless components, circumspection was made to alleviate the contributions of other factors in their demonstrated performance. All testing was conducted using the same non-associated equipment for each round of testing. The only components that differed were the units under test (wireless adapter cards and corresponding access points). Therefore, none of the performance gains realized were due to computer or operating system differences.

The following paragraphs detail the specific components, testing methodology, geography and results associated with this evaluation.

A. ANALYSIS OF EQUIPMENT

The equipment utilized in the evaluation was separated into two categories, associated and non-associated equipment. Non-associated equipment is the equipment involved in the evaluation that was common to all tested components. This equipment includes both hardware and software. Associated equipment specifies the devices being evaluated for performance.

1. Non-associated Equipment

In order to ensure consistency, the same computer equipment was used for testing each of the wireless components that were evaluated. The results of throughput testing indicated that different wireless components produced a wide variation of results. The purpose of maintaining consistency with the non-associated equipment was to ensure that all the wireless components were effected similarly. Therefore, the differences in performance were characteristic of the wireless component under test. To provide the means to accurately reproduce the testing, each of the non-associated devices is described below. Figure 5.1 illustrates a typical test configuration.

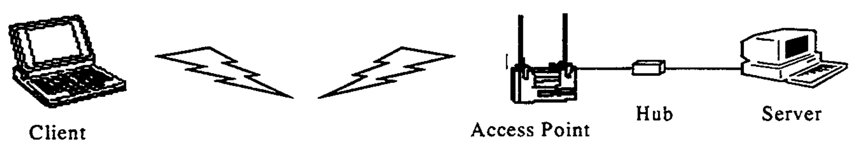


Figure 5.1 Typical Test Configuration

- **Server:** Dell Dimension XPS R400 desktop computer
  - Pentium II processor operating at 400 MHz
  - 128 MB random access memory (RAM)
  - Windows NT (version 4.0) operating system
  - FTP Server War FTP Daemon (version 1.70)
- **Client:** Dell Latitude CP laptop computer
  - Pentium processor operating at 233 MHz with MMX™
  - 32 MB random access memory (RAM)
  - Windows 98 operating system

- FTP Client WS_FTP95 LE (version 4.60)

- **Hub:** 10Mbps Kingston EtherRX Soho Hub

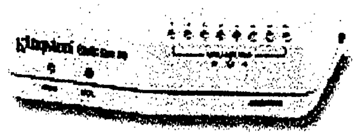


Figure 5.2: Kingston Ethernet Hub From Ref. [30]

2. Associated Equipment

The associated equipment tested is listed in Table 5.1. The test included the PCMCIA adapter cards and the corresponding access points.

Manufactures	**Lucent Technologies**	**Aironet™**
IEEE 802.11 Compliant	WaveLan®	
IEEE 802.11b Compliant	WaveLan® TURBO BRONZE	4800 Series TURBO DS

Table 5.1: Evaluated Wireless Components

B. EVALUATION TOOLS

Both Lucent Technologies and Aironet provided proprietary diagnostic tools, which were useful in the evaluation of their products. These diagnostic tools are typically used to provide a RF network coverage assessment to determine or optimize placement of the wired and wireless components. The diagnostic tools also provided a means to verify the quality of communications between the adapter card and the access point.

1. WaveMANAGER/CLIENT IEEE Program

The Lucent Technology WaveMANAGER/CLIENT diagnostic tool, shown in Fig. 5.3, was used to judge the radio connection, data transmission rate, signal impact and SNR (in dB) between the Lucent adapter cards and the WavePOINT-II access point. These items are included in the Excel worksheet under the columns Quality and dB.

The following abbreviations are used in the Quality column of the worksheet:

- Connection: G = Good
  A = Adequate
- Transmission Rate: H = High
  S = Standard
- Impact: E = Excellent
  N = Normal

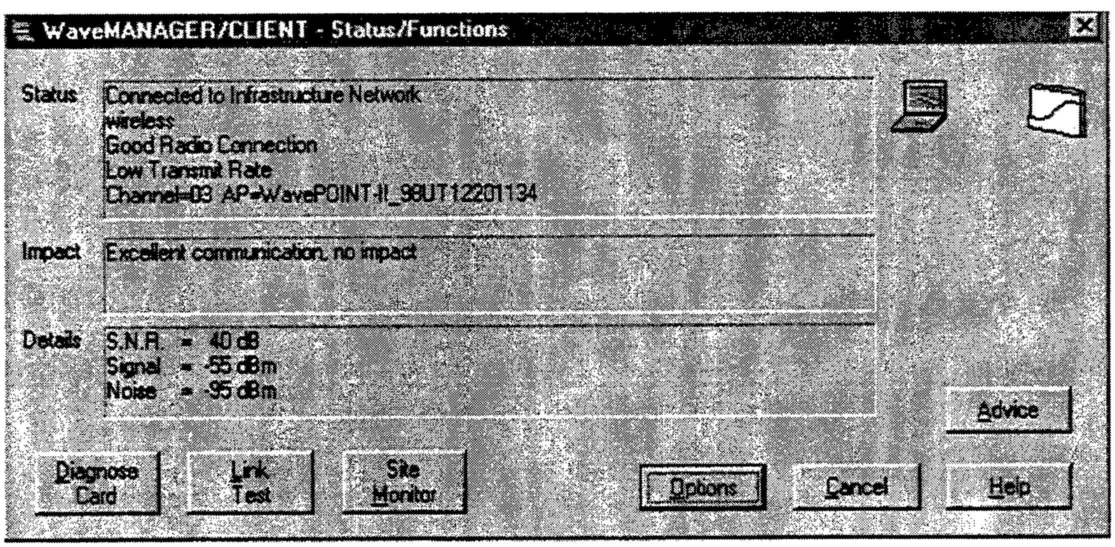


Figure 5.3: WaveMANAGER/CLIENT Diagnostic Tool From Ref. [31]

2. LinkScope

The Aironet LinkScope diagnostic tool, shown in Fig. 5.4, was used to judge signal strength and quality between the Aironet 4800 Series TURBO DS access point and adapter cards. LinkScope, although easy to use, is not very helpful in the evaluation. The sporadic signal conditions experienced while testing made this tool ineffective. The access point and adapter card lost association repeatedly over the course of testing. Each lost association required that the testing be suspended and the FTP connection be reestablished.

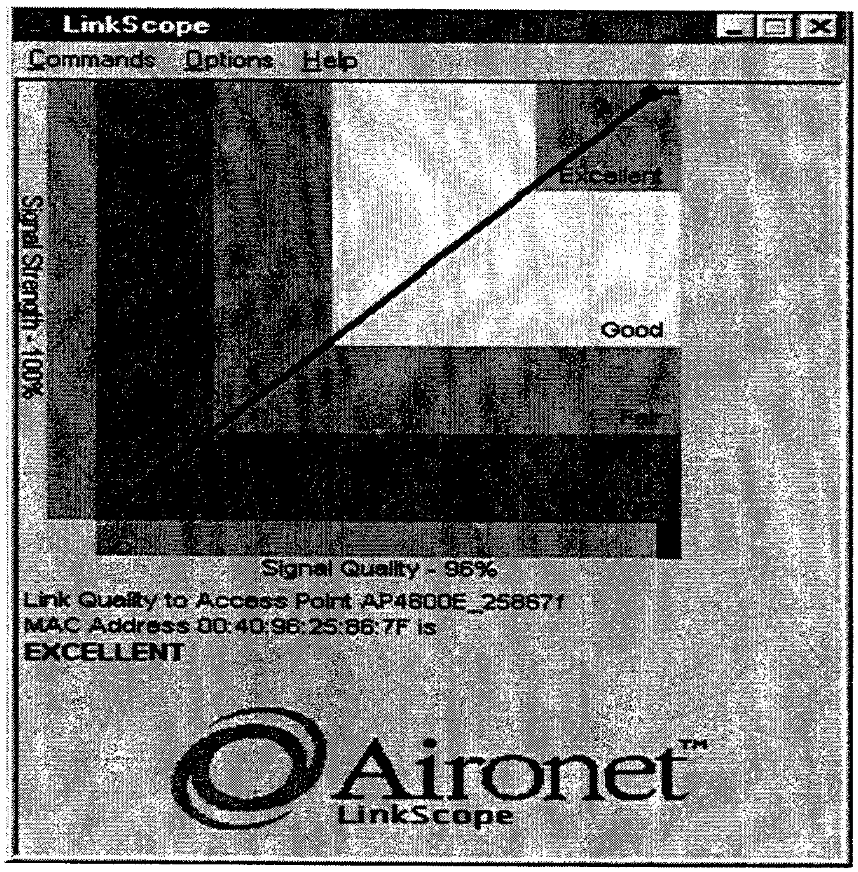


Figure 5.4: Aironet LinkScope Diagnostic Tool From Ref. [32]

C. TEST PROCEDURES

The access point and the adapter cards were tested outdoors. The desktop computer (server) and the hub remained indoors. A 100 ft 10baseT cable was used to connect the hub to the access point. Testing was conducted in two phases, line-of-sight and non-line-of-sight. Each wireless component was tested in both phases and each phase consisted of six passes. The file transfer protocol (FTP) program cited above was used to transfer a 5.31 Mbyte bitmap file between the client and server. The FTP program provided a throughput calculation based on the file size and transfer time. The transfer was repeated at intervals of ten feet. Fig. 5.5 is provided to illustrate the geography of the area where the test was performed.

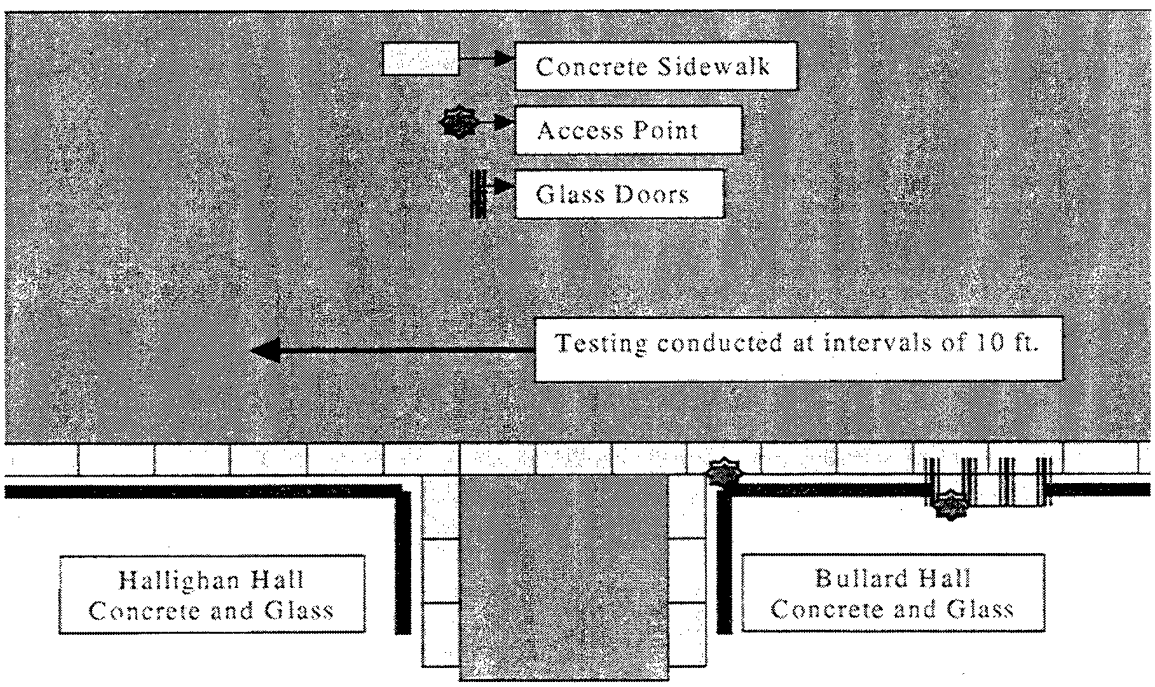


Figure 5.5: Testing Geography

There were a total of six passes that included three passes from client-to-server and three passes from server-to-client. The three passes for each transmission was averaged and plotted in the Excel graphs presented later. At each interval, the client was positioned for the maximum signal level at that location. Throughout the testing, only two applications were running, FTP and the diagnostic program associated with the unit under test. The adapter cards and the access points were locked in the maximum data rate setting. The maximum data rate for the turbo cards was 11 Mbps and 2 Mbps for the non-turbo card. Testing was concluded when communications were no longer possible at the test range.

D. EVALUATED COMPONENTS

1. Lucent Technologies WaveLAN IEEE (Non-turbo) Components

As mentioned earlier in the chapter, the WaveLan PCMCIA adapter, produced by Lucent Technologies, was chosen to be the representative IEEE 802.11 compliant component for this testing. The WaveLAN IEEE adapter card is pictured in Fig. 5.6 along with a WavePOINT-II Access Point and the WaveLan Range Extender Antenna. The adapter card's characteristics are described below.

- **Adapter Type:** DSSS, IEEE 802.11 Compliant
- **Advertised Range at Data Rate:**

	2 Mbps	1 Mbps
Open Environment	1200 ft	1400 ft
Semi-Open Environment	550 ft	650 ft

- **Maximum Data Rate:** 2 Mbps in high signal strength

		1 Mbps in low signal strength	
•	**Nominal Output Power:**	32 mW	
•	**Current Draw Characteristics:**	Transmit	330 mA
		Receive	280 mA
		Sleep	9 mA

Figure 5.6: Lucent Technologies WaveLAN IEEE Components

- **Throughput**

The measured data throughput is presented in two forms, first a Microsoft Excel worksheet and secondly, a Microsoft Excel graph. Table 5.2 shows the results of the throughput testing conducted at various distances from the access point for the line-of-sight scheme. Distance values are in feet and throughput values for all passes are in Mbps. Fig. 5.7 is the graphical representation of the results. Table 5.3 and Fig. 5.8 show the results of the throughput testing conducted for the non-line-of-sight scheme.

Lucent Technologies White IEEE 802.11
Access Point and Mobile Fixed Standard Data Rate
Testing Conducted Line-of-Sight

	Laptop to Desktop				Desktop to Laptop					
Distance	1st Pass	2nd Pass	3rd Pass	Average	1st Pass	2nd Pass	3rd Pass	Average	dB	Quality
10	1.37	1.38	1.38	1.38	1.67	1.68	1.60	1.65	53	GSE
20	1.38	1.38	1.38	1.38	1.68	1.69	1.67	1.68	47	GSE
30	1.37	1.37	1.36	1.37	1.64	1.65	1.56	1.62	40	GSE
40	1.36	1.37	1.38	1.37	1.68	1.68	1.67	1.68	41	GSE
50	1.38	1.37	1.38	1.38	1.67	1.65	1.68	1.67	42	GSE
60	1.38	1.38	1.38	1.38	1.68	1.67	1.64	1.66	41	GSE
70	1.36	1.37	1.36	1.36	1.57	1.59	1.60	1.59	41	GSE
80	1.35	1.36	1.36	1.36	1.47	1.52	1.55	1.51	40	GSE
90	1.36	1.35	1.35	1.35	1.61	1.54	1.46	1.54	39	GSE
100	1.37	1.36	1.36	1.36	1.53	1.60	1.59	1.57	38	GSE
110	1.37	1.36	1.37	1.37	1.61	1.62	1.56	1.60	37	GSE
120	1.37	1.37	1.37	1.37	1.58	1.63	1.68	1.63	36	GSE
130	1.35	1.36	1.36	1.36	1.47	1.47	1.46	1.47	37	GSE
140	1.36	1.35	1.36	1.36	1.49	1.46	1.48	1.48	35	GSE
150	1.36	1.36	1.36	1.36	1.45	1.48	1.55	1.49	36	GSE
160	1.36	1.36	1.34	1.35	1.46	1.42	1.54	1.47	35	GSE
170	1.35	1.36	1.35	1.35	1.49	1.56	1.60	1.55	35	GSE
180	1.37	1.37	1.37	1.37	1.68	1.63	1.68	1.66	34	GSE
190	1.36	1.38	1.37	1.37	1.67	1.67	1.65	1.66	30	GSE
200	1.37	1.36	1.36	1.36	1.68	1.64	1.68	1.67	31	GSE
210	1.36	1.36	1.36	1.36	1.66	1.63	1.68	1.66	30	GSE
220	1.35	1.36	1.37	1.36	1.63	1.66	1.67	1.65	28	GSE
230	1.34	1.36	1.36	1.35	1.65	1.64	1.67	1.65	30	GSE
240	1.37	1.35	1.36	1.36	1.61	1.67	1.63	1.64	28	GSE
250	1.36	1.36	1.37	1.36	1.65	1.67	1.67	1.66	29	GSE
260	1.31	1.34	1.33	1.33	1.65	1.56	1.62	1.61	26	GSN
270	1.32	1.33	1.34	1.33	1.49	1.58	1.52	1.53	22	GSN
280	1.34	1.34	1.35	1.34	1.53	1.53	1.61	1.56	25	GSN
290	1.30	1.32	1.33	1.32	1.56	1.58	1.59	1.58	22	GSN
300	1.35	1.35	1.35	1.35	1.60	1.63	1.63	1.62	26	GSN
310	1.31	1.34	1.33	1.33	1.48	1.62	1.61	1.57	20	ASN
320	1.32	1.34	1.34	1.33	1.62	1.55	1.60	1.59	23	GSN
330	1.32	1.33	1.34	1.33	1.58	1.59	1.64	1.60	23	GSN
340	1.34	1.34	1.35	1.34	1.57	1.61	1.63	1.60	23	GSN
350	1.29	1.29	1.30	1.29	1.57	1.53	1.54	1.55	19	ASN
360	1.31	1.34	1.29	1.31	1.58	1.59	1.61	1.59	22	GSN
370	1.30	1.31	1.32	1.31	1.55	1.57	1.49	1.54	19	ASN
380	1.35	1.34	1.32	1.34	1.64	1.64	1.60	1.63	21	GSN
390	1.28	1.31	1.32	1.30	1.54	1.49	1.56	1.53	20	ASN
400	1.26	1.27	1.27	1.27	1.46	1.59	1.54	1.53	17	ASN
410	1.20	1.23	1.24	1.22	1.48	1.43	1.51	1.47	16	ASN
420	1.29	1.33	1.32	1.31	1.56	1.57	1.56	1.56	18	ASN

Table 5.2: Lucent Technologies White IEEE 802.11 Line-of-Sight

Lucent Technologies White IEEE 802.11 (Cont.)
Access Point and Mobile Fixed Standard Data Rate
Testing Conducted Line-of-Sight

	Laptop to Desktop				Desktop to Laptop					
Distance	1st Pass	2nd Pass	3rd Pass	Average	1st Pass	2nd Pass	3rd Pass	Average	dB	Quality
430	1.30	1.31	1.30	1.30	1.42	1.56	1.49	1.49	16	ASN
440	1.17	1.23	1.25	1.22	1.27	1.36	1.30	1.31	16	ASN
450	1.22	1.23	1.24	1.23	1.38	1.38	1.44	1.40	17	ASN
460	1.29	1.29	1.29	1.29	1.52	1.60	1.59	1.57	18	ASN
470	1.31	1.29	1.30	1.30	1.43	1.40	1.42	1.42	18	ASN
480	1.31	1.26	1.30	1.29	1.36	1.34	1.44	1.38	19	ASN
490	1.22	1.23	1.28	1.24	1.33	1.25	1.30	1.29	17	ASN
500	1.22	1.27	1.24	1.24	1.22	1.30	1.29	1.27	17	ASN
510	1.27	1.27	1.28	1.27	1.36	1.37	1.37	1.37	17	ASN
520	1.27	1.31	1.26	1.28	1.44	1.49	1.46	1.46	19	ASN
530	1.30	1.32	1.31	1.31	1.42	1.61	1.55	1.53	20	ASN
540	1.13	1.30	1.28	1.24	1.44	1.55	1.59	1.53	19	ASN
550	1.31	1.31	1.30	1.31	1.65	1.63	1.45	1.58	18	ASN

Table 5.2: Lucent Technologies White IEEE 802.11 Line-of-Sight (Cont.)

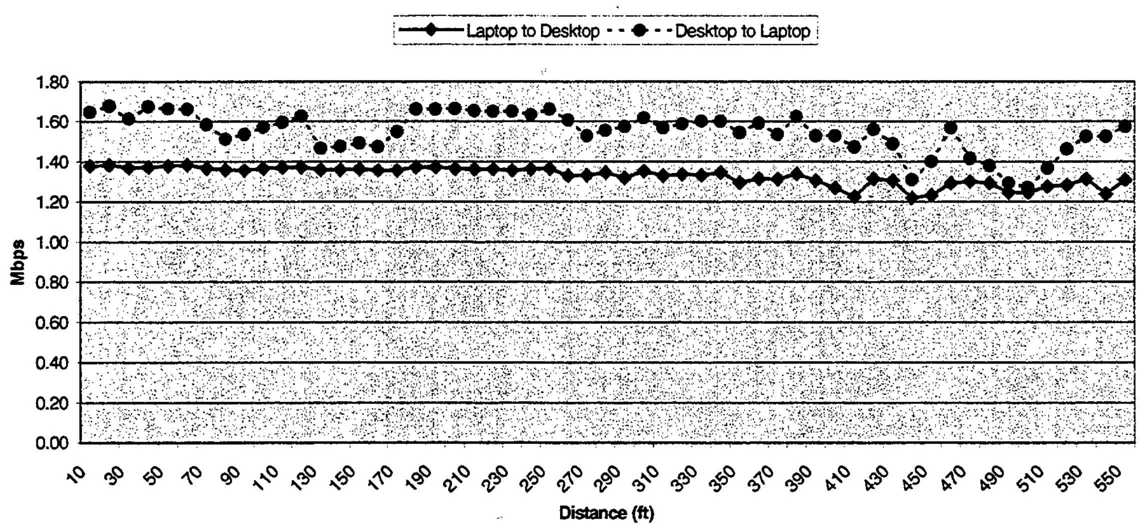


Figure 5.7: Lucent Technology White IEEE 802.11 Line-of-Sight

Lucent Technologies White IEEE 802.11

Access Point and Mobile Fixed Standard Data Rate

Testing Conducted Non-Line-of-Sight

	Laptop to Desktop				Desktop to Laptop					
Distance	1st Pass	2nd Pass	3rd Pass	Average	1st Pass	2nd Pass	3rd Pass	Average	dB	Quality
10	1.37	1.37	1.37	1.37	1.60	1.53	1.60	1.58	38	GSE
20	1.30	1.31	1.31	1.31	1.50	1.46	1.59	1.52	28	GSE
30	1.31	1.30	1.30	1.30	1.48	1.54	1.51	1.51	28	GSE
40	1.32	1.30	1.29	1.30	1.47	1.56	1.48	1.50	26	GSE
50	1.29	1.36	1.26	1.30	1.52	1.47	1.49	1.49	21	GSN
60	1.25	1.26	1.27	1.26	1.43	1.44	1.47	1.45	20	ASN
70	1.27	1.29	1.26	1.27	1.41	1.42	1.43	1.42	18	ASN
80	1.29	1.30	1.32	1.30	1.47	1.44	1.39	1.43	17	ASN
90	1.27	1.28	1.29	1.28	1.36	1.48	1.45	1.43	17	ASN
100	1.28	1.28	1.25	1.27	1.46	1.32	1.47	1.42	17	ASN
110	1.28	1.28	1.29	1.28	1.45	1.43	1.43	1.44	17	ASN
120	1.29	1.28	1.26	1.28	1.46	1.21	1.39	1.35	16	ASN
130	1.27	1.28	1.30	1.28	1.43	1.50	1.46	1.46	16	ASN
140	1.25	1.28	1.26	1.26	1.26	1.18	1.28	1.24	15	ASN
150	1.25	1.26	1.25	1.25	1.18	1.20	1.14	1.17	13	ASR
160	1.23	1.25	1.25	1.24	1.33	1.25	1.26	1.28	12	ASR
170	1.23	1.24	1.24	1.24	1.06	1.16	1.23	1.15	11	ASR
180	1.27	1.28	1.26	1.27	1.18	1.16	1.26	1.20	14	ASR
190	1.30	1.28	1.27	1.28	1.20	1.34	1.32	1.29	13	ASR
200	1.28	1.26	1.29	1.28	1.29	1.36	1.33	1.33	14	ASR
210	1.30	1.30	1.29	1.30	1.45	1.45	1.40	1.43	15	ASR
220	1.17	1.26	1.26	1.23	1.18	1.33	1.30	1.27	11	ASR
230	1.17	1.20	1.24	1.20	1.05	1.05	1.02	1.04	10	ASR
240	1.17	1.10	1.19	1.15	0.96	0.97	0.68	0.87	8	ASR
250	1.03	1.21	1.23	1.16	0.97	1.13	0.74	0.95	8	ASR
260	1.21	1.18	1.20	1.20	1.03	1.07	0.99	1.03	8	ASR
270	1.13	1.11	1.13	1.12	0.87	0.98	0.78	0.88	8	ASR
280	1.20	1.16	1.15	1.17	0.81	0.97	0.87	0.88	7	ASR
290	0.93	0.82	1.02	0.92	0.43	0.58	0.73	0.58	7	ASR
300	1.16	1.19	1.18	1.18	1.17	1.10	1.10	1.12	8	ASR
310	1.20	1.20	1.15	1.18	0.95	0.77	0.87	0.86	8	ASR
320	1.23	1.21	1.22	1.22	1.27	1.26	1.16	1.23	9	ASR
330	1.18	1.18	1.21	1.19	0.85	0.98	1.05	0.96	8	ASR
340	1.22	1.14	1.17	1.18	1.05	0.95	0.98	0.99	8	ASR
350	1.21	1.20	1.16	1.19	1.04	1.06	0.88	0.99	8	ASR

Table 5.3: Lucent Technologies White IEEE 802.11 Non-Line-of-Sight

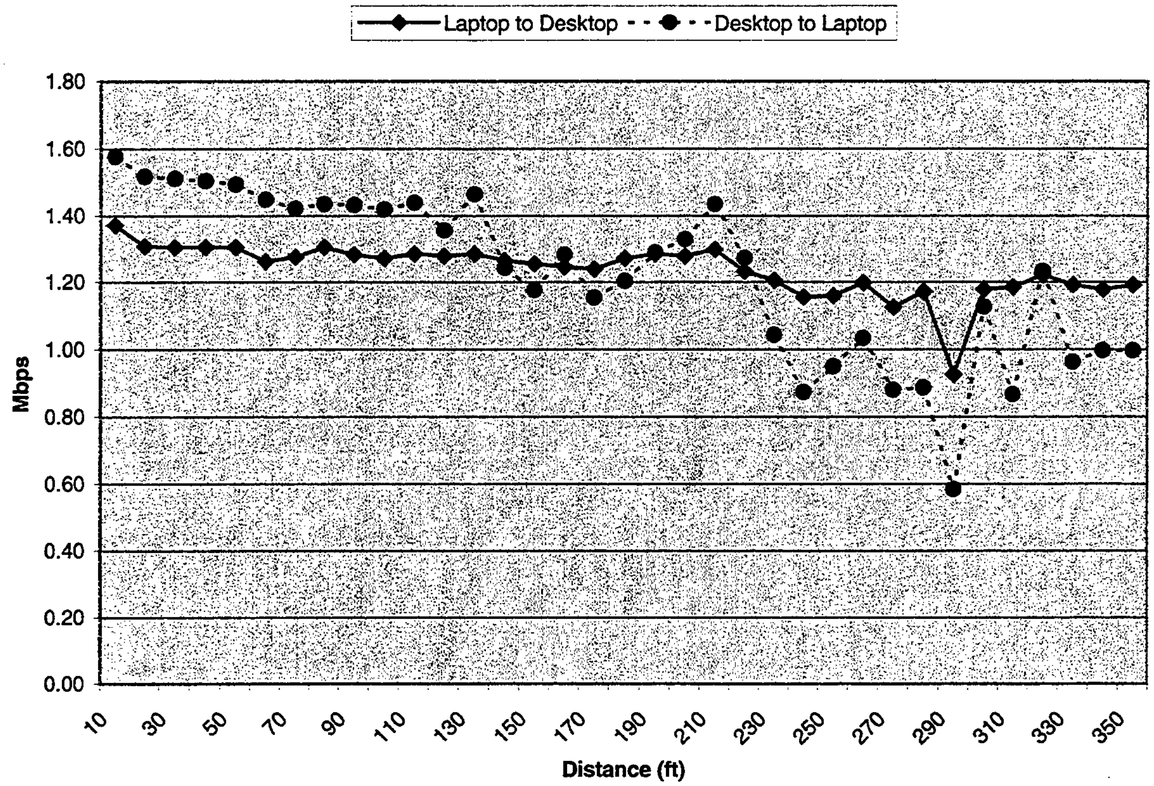


Figure 5.8: Lucent Technology White IEEE 802.11 Non-Line-of-Sight

2. Lucent Technologies WaveLAN IEEE 802.11 Turbo Card

The WaveLAN IEEE 802.11 Turbo card is pictured in Fig. 5.9. The same access point and range extender antenna was used for the Turbo card testing.

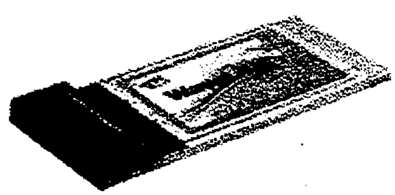


Figure 5.9: Lucent Bronze Turbo From Ref. [33]

- **Adapter Type:** DSSS, IEEE 802.11b Compliant
- **Advertised Range at Data Rate:**

	11 Mbps	5.5 Mbps	2 Mbps	1Mbps
Open Environment	400 ft	650 ft	1300 ft	1750 ft
Semi-Open Environment	130 ft	180 ft	300 ft	375 ft

- **Maximum Data Rate:** Dependent on signal quality (Auto Mode)
- **Nominal Output Power:** 32 mW
- **Current Draw Characteristics:**

Transmit	330 mA
Receive	280 mA
Sleep	9 mA

- **Throughput**

Table 5.4 and Fig 5.10 show the results of the throughput testing conducted at various distances from the access point for the Lucent Technologies Turbo line-of-sight scheme. Table 5.5 and Fig. 5.11 present the results of the throughput testing conducted for the non-line-of-sight scheme.

Lucent Technologies Bronze Turbo										
Access Point and Mobile Fixed High Data Rate										
Testing Conducted Line-of-Sight										
	Laptop to Desktop				Desktop to Laptop					
Distance	1st Pass	2nd Pass	3rd Pass	Average	1st Pass	2nd Pass	3rd Pass	Average	dB	Quality
10	3.01	3.04	3.03	3.03	4.44	4.38	4.46	4.43	52	GHE
20	3.01	3.03	3.03	3.02	4.39	4.42	4.34	4.38	51	GHE
30	2.66	2.76	2.54	2.65	3.45	3.84	3.92	3.74	35	GHE
40	2.84	2.89	2.91	2.88	3.67	3.73	4.16	3.85	42	GHE
50	2.77	2.76	2.84	2.79	3.75	3.94	4.17	3.95	44	GHE
60	2.86	2.88	2.90	2.88	3.84	4.31	4.16	4.10	42	GHE
70	2.83	2.86	2.92	2.87	3.94	4.18	4.24	4.12	42	GHE
80	2.77	2.82	2.93	2.84	3.64	3.78	4.00	3.81	40	GHE
90	2.86	2.78	2.80	2.81	3.67	3.90	3.69	3.75	41	GHE
100	2.73	2.83	2.96	2.84	3.70	3.80	4.04	3.85	40	GHE
110	2.73	2.55	2.83	2.70	4.04	3.90	3.85	3.93	39	GHE
120	2.12	2.28	2.31	2.24	3.55	3.97	4.12	3.88	38	GHE
130	1.82	2.23	2.25	2.10	3.18	3.75	3.15	3.36	33	GHE
140	2.69	2.76	2.81	2.75	3.41	3.53	3.46	3.47	33	GHE
150	2.78	2.71	2.86	2.78	3.39	4.02	3.76	3.72	34	GHE
160	2.65	2.79	2.78	2.74	3.94	3.14	3.84	3.64	34	GHE
170	2.80	2.69	2.83	2.77	3.21	3.47	3.78	3.49	30	GHE
180	2.21	2.35	2.49	2.35	3.67	3.64	4.03	3.78	29	GHE
190	2.62	2.60	2.75	2.66	4.12	4.07	3.61	3.93	29	GHE
200	2.62	2.55	2.52	2.56	3.73	3.80	3.79	3.77	30	GHE
210	2.38	2.47	2.19	2.35	3.83	3.99	4.11	3.98	28	GHE
220	2.21	1.97	1.83	2.00	3.57	3.53	3.40	3.50	25	GHN
230	2.41	2.35	2.31	2.36	3.95	3.69	4.02	3.89	28	GHE
240	2.60	2.69	2.70	2.66	3.50	3.84	3.94	3.76	29	GHE
250	2.58	2.66	2.70	2.65	4.21	4.24	4.00	4.15	29	GHE
260	2.76	2.63	2.87	2.75	4.03	4.21	3.99	4.08	30	GHE
270	2.13	1.89	2.21	2.08	3.87	3.75	3.70	3.77	27	GHE
280	2.59	2.39	2.33	2.44	3.80	3.23	3.95	3.66	26	GHE
290	2.65	2.66	2.37	2.56	4.02	3.94	3.65	3.87	26	GHE
300	2.58	2.44	2.52	2.51	3.48	3.93	3.89	3.77	27	GHE
310	2.66	2.65	2.61	2.64	3.25	4.09	3.98	3.77	26	GHE
320	2.65	2.71	2.58	2.65	3.94	3.82	4.22	3.99	26	GHE
330	2.66	2.58	2.33	2.52	4.04	3.74	4.10	3.96	24	GHN
340	1.74	1.92	2.04	1.90	3.26	3.83	4.23	3.77	22	GHN
350	2.48	2.59	2.04	2.37	3.39	2.70	3.46	3.18	22	GHN
360	1.05	1.57	1.46	1.36	1.71	1.35	1.47	1.51	17	AHN

Table 5.4: Lucent Technology Bronze Turbo IEEE 802.11b Line-of-Sight

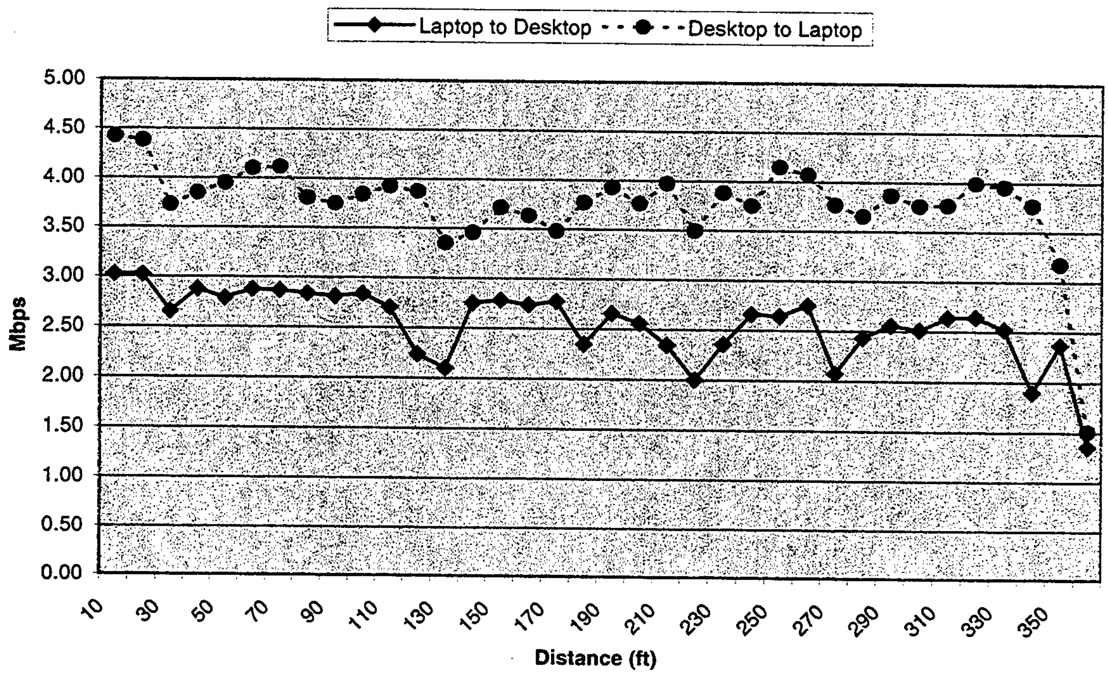


Figure 5.10: Lucent Technology Bronze Turbo IEEE 802.11b Line-of-Sight

Lucent Technologies Bronze Turbo Access Point and Mobile Fixed Standard Data Rate Testing Conducted Non-Line-of-Sight										
	Laptop to Desktop				Desktop to Laptop					
Distance	1st Pass	2nd Pass	3rd Pass	Average	1st Pass	2nd Pass	3rd Pass	Average	dB	Quality
10	2.78	2.85	2.71	2.78	3.08	3.79	2.96	3.28	36	GHE
20	1.76	1.52	2.40	1.89	2.36	3.06	2.40	2.61	27	GHE
30	1.12	1.78	1.44	1.45	2.94	1.89	1.84	2.22	24	GHN
40	2.84	2.67	1.90	2.47	1.78	3.28	3.39	2.82	26	GHE
50	2.33	1.71	1.72	1.92	1.34	2.15	1.88	1.79	22	GHN
60	2.16	2.67	1.92	2.25	2.73	2.25	3.51	2.83	24	GHN
70	2.17	1.85	1.16	1.73	3.32	2.30	2.69	2.77	23	GHN
80	1.73	1.91	2.60	2.08	1.52	3.20	1.91	2.21	22	GHN
90	1.27	1.08	1.29	1.21	0.93	0.78	0.89	0.87	15	AHR

Table 5.5: Lucent Technologies Bronze Turbo Non-Line-of-Sight

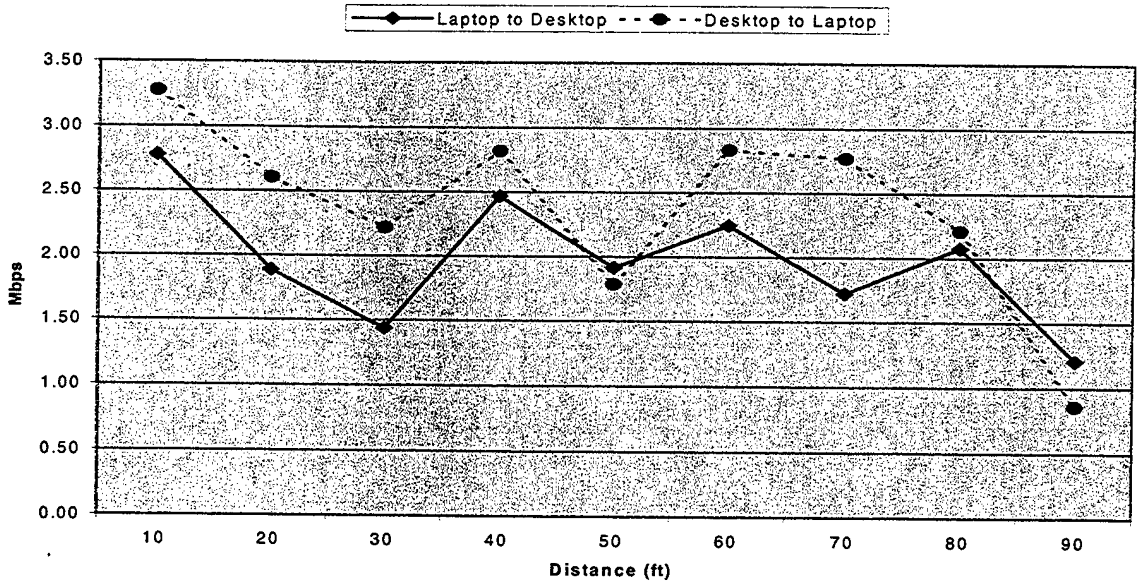


Figure 5.11: Lucent Technology Bronze Turbo IEEE 802.11b Non-Line-of-Sight

3. Aironet Wireless LAN Adapter and Access Point

The Aironet Turbo DS access point and adapter cards are pictured in Fig. 5.12.

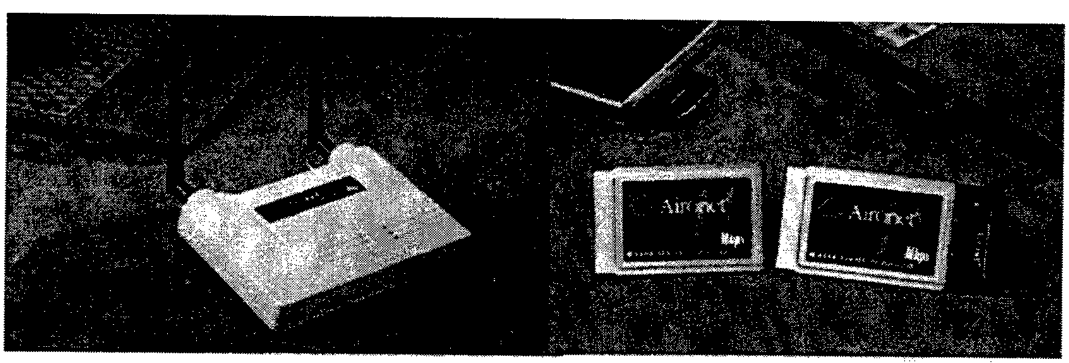


Figure 5.12: Aironet Turbo DS Access Point and Adapter Cards From Ref. [34]

- **Adapter Type:** DSSS, IEEE 802.11b Compliant
- **Advertised Range at Data Rate:** 11 Mbps 1Mbps

	11 Mbps	1Mbps
Open Air Environment	500 ft	1800 ft

Indoors	100 ft	350 ft

- **Maximum Data Rate:** Dependent on signal quality (Auto Mode)
- **PC Card Transmit Power:** 100 mW
- **Current Draw Characteristics:**

Transmit	490 mA
Receive	280 mA
Sleep	5 mA

- **Throughput**

Table 5.6 and Fig 5.13 show the results of the throughput testing conducted at various distances from the access point for the Aironet Turbo DS line-of-sight scheme. Table 5.7 and Fig. 5.14 present the results of the throughput testing conducted for the non-line-of-sight scheme.

Aironet™ 4800 Series Turbo DS								
Access Point and Mobile Fixed High Data Rate								
Testing Conducted Line-of-Sight								
	Laptop to Desktop				Desktop to Laptop			
Distance	1st Pass	2nd Pass	3rd Pass	Average	1st Pass	2nd Pass	3rd Pass	Average
10	3.61	3.31	4.13	3.68	3.44	3.42	3.42	3.43
20	3.56	3.67	3.53	3.59	3.66	3.66	3.55	3.62
30	3.44	4.00	3.53	3.66	3.32	3.20	2.99	3.17
40	3.74	4.70	4.28	4.24	3.38	3.32	3.41	3.37
50	4.35	3.74	4.66	4.25	3.39	3.40	3.31	3.37
60	3.77	3.82	4.12	3.90	3.24	3.40	3.36	3.33
70	4.66	3.59	3.84	4.03	3.43	3.43	3.33	3.40
80	4.09	3.99	3.93	4.00	3.35	3.16	3.41	3.31
90	3.22	3.87	3.67	3.59	3.39	3.35	3.36	3.37
100	3.21	4.02	3.40	3.54	2.90	3.42	2.58	2.97
110	3.32	3.12	3.77	3.40	3.19	3.56	3.13	3.29
120	4.28	3.68	3.57	3.84	3.08	1.71	2.98	2.59
130	2.82	3.65	3.87	3.45	2.77	2.66	2.95	2.79
140	3.59	3.63	4.25	3.82	3.04	2.72	3.17	2.98
150	2.89	2.82	2.66	2.79	3.28	2.36	2.74	2.79
160	3.74	4.10	3.76	3.87	3.34	3.26	3.44	3.35
170	3.37	3.69	3.85	3.64	3.14	2.58	3.01	2.91
180	1.74	2.90	2.45	2.36	2.54	2.45	3.10	2.70
190	3.35	3.45	3.31	3.37	3.09	2.96	3.00	3.02
200	2.31	3.33	3.62	3.09	2.49	1.51	2.63	2.21
210	3.07	1.62	3.22	2.64	2.75	2.93	2.85	2.84
220	2.84	3.00	3.00	2.95	3.24	3.33	2.24	2.94
230	2.68	3.48	3.13	3.10	2.04	2.28	1.82	2.05
240	2.78	2.21	1.95	2.31	2.07	2.53	2.40	2.33
250	3.48	2.99	3.09	3.19	1.71	2.50	2.91	2.37
260	3.87	3.55	3.78	3.73	2.35	1.10	0.56	1.34
270	3.20	3.78	3.32	3.43	3.12	3.09	3.14	3.12
280	1.19	1.97	2.93	2.03	0.97	1.13	0.98	1.03
290	3.16	3.49	2.14	2.93	2.30	2.32	2.55	2.39
300	3.26	3.71	3.79	3.59	2.60	2.61	2.82	2.68
310	3.02	3.34	4.27	3.54	3.12	2.32	2.94	2.79
320	4.23	3.43	4.02	3.89	3.05	3.09	2.79	2.92
330	3.78	3.78	3.88	3.81	3.01	2.56	3.00	2.86
340	3.55	4.08	3.81	3.81	3.07	3.19	3.05	3.10
350	3.91	3.64	4.50	4.02	3.06	2.94	3.10	3.03
360	2.34	3.52	3.80	3.22	2.39	2.86	1.32	2.19
370	4.06	3.54	3.44	3.68	2.96	3.00	2.95	2.97
380	3.28	3.51	3.46	3.42	1.52	2.13	1.34	1.66
390	2.81	3.76	2.88	3.15	2.44	2.35	1.71	2.17

Table 5.6: Aironet Turbo DS IEEE 802.11b Line-of-Sight

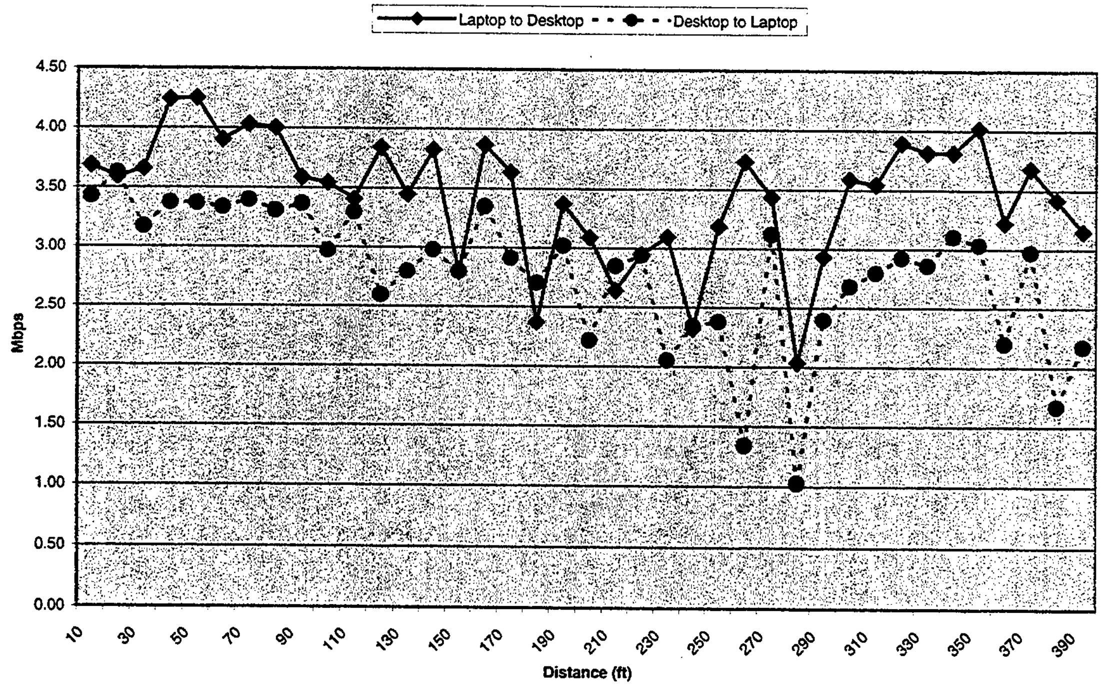


Figure 5.13: Aironet Turbo DS IEEE 802.11b Line-of-Sight

Aironet™ 4800 Series Turbo DS								
Access Point and Mobile Fixed High Data Rate								
Testing Conducted Non-Line-of-Sight								
	Laptop to Desktop				Desktop to Laptop			
Distance	1st Pass	2nd Pass	3rd Pass	Average	1st Pass	2nd Pass	3rd Pass	Average
10	3.80	3.49	4.18	3.82	3.31	3.28	3.41	3.33
20	3.66	2.88	3.00	3.18	2.01	2.24	2.61	2.29
30	4.22	3.32	3.81	3.78	3.48	3.54	3.69	3.57
40	3.28	3.60	3.29	3.39	3.54	3.48	3.50	3.51
50	3.19	3.94	3.73	3.62	1.52	2.18	2.15	1.95
60	2.75	2.37	2.60	2.57	2.65	2.76	1.56	2.32
70	2.97	2.82	2.77	2.85	1.04	1.66	1.94	1.55
80	3.09	3.44	3.74	3.42	3.32	2.75	2.81	2.96
90	2.21	2.76	2.03	2.33				

Table 5.7: Aironet Turbo DS IEEE 802.11b Non-Line-of-Sight

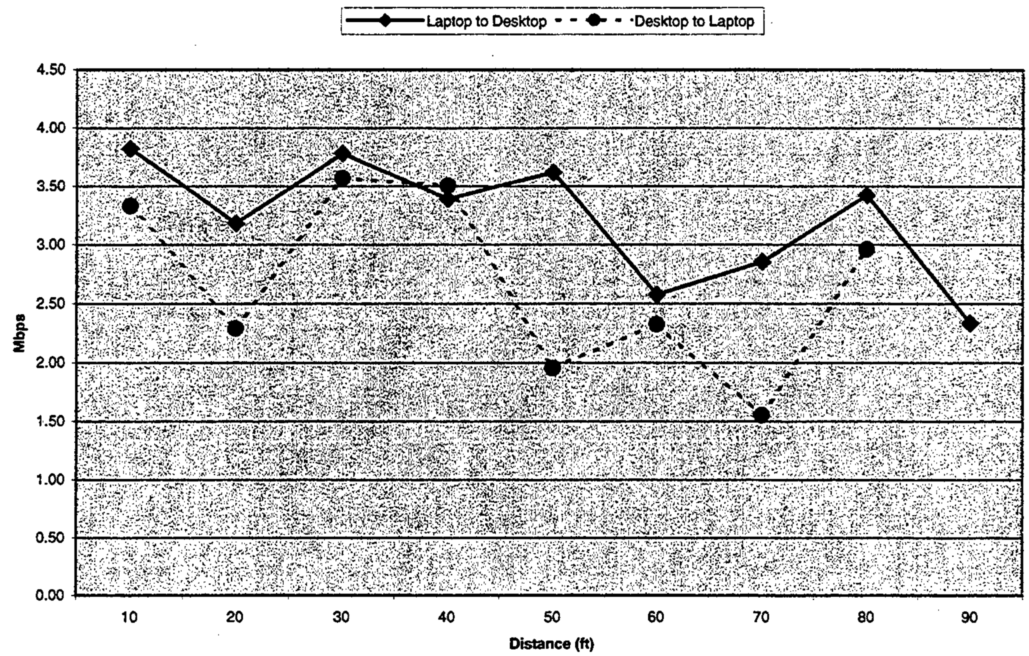


Figure 5.14: Aironet Turbo DS IEEE 802.11b Non-Line-of-Sight

E. DISCUSSION OF RESULTS

The results of the test indicate that the Lucent Technologies WaveLAN Turbo components offered a more consistent performance than the Aironet Turbo DS components did. The actual measured throughput of both versions of the turbo cards was less than 30% of the advertised, 11 Mbps rate. The Lucent Technologies turbo card measured approximately 29% of its advertised data rate compare to Aironet's 28% for LOS and approximately 20% and 27% respectfully, for NLOS. Even though the data rates are discouraging when compare to the advertised rates, the Lucent turbo card still showed an

increase of 220% over the IEEE 802.11 compliant non-turbo card for LOS and a gain of 177% for NLOS. The measure ranges were much more in line with the published ranges

Recall that the IEEE 802.11b high speed standard ensures backward compatibility with the original IEEE 802.11 standard and that this test was conducted to evaluate the performance of the turbo cards at the highest data rate possible. The testing data would have yielded much different results if the components were afforded their full range of operability.

VI. CONCLUSIONS

The goal of this thesis was to evaluate several commercially available wireless components that operate on the principal of direct sequence spread spectrum. A comparative analysis was conducted between several wireless components, which included a comparison between line-of-sight and non-line-of-sight performance. The analysis also included a comparison between a 2 Mbps IEEE 802.11 compliant component and several IEEE 802.11b compliant components, operating at a data rate of 11 Mbps.

A. DISCUSSION

While spread spectrum techniques are good for avoiding interference, there is a trade-off. The more interference, the more aggressive the steps that must be taken to avoid it. Direct sequence systems are very robust but they do have drawbacks. As signal interference grows and the SNR decreases, data rate or distance will also have to decrease. The results described in Chapter V demonstrate that the IEEE 802.11b compliant components offer single client throughput of approximately twice that of the previous IEEE standard but at a significantly reduced range.

1. Lucent Technologies WaveLan Pros and Cons

The Lucent Technologies WaveLan components offer several attractive features. The first is the ability to upgrade the access point. The same access point was used to test both the IEEE 802.11 and IEEE 802.11b compliant components. The access point is equipped with two PCMCIA slots. All that was required to upgrade to the IEEE 802.11b

standard was a turbo card in the PCMCIA slot and some software upgrades. The foresight on the part of Lucent to produce equipment that would function with expected future advances makes the WaveLan devices very appealing.

The second attractive feature is the ability to locate the Range Extender Antenna up to four feet away from the access point. This allows for the mounting of the access point in a convenient location while being able to better position the antenna in order to achieve the maximum signal reception.

The only drawback encountered while testing the Lucent products was with the software installation. In order to upgrade to the high speed turbo cards, new device drivers and network adapters had to be installed along with upgrades to the WaveMANAGER/CLIENT IEEE diagnostic tool, WaveMANAGER AP, and WaveLAN IEEE PC card firmware.

2. Aironet 4800 Series TURBO DS Pros and Cons

The Aironet components also offer several attractive features. The first is the ability to easily set up the access point. Making changes to the network and radio settings was very easy. With a serial cable connected to the Console/RS-232C port, it was possible to access the Console program to make changes to the configuration, set filters, run diagnostics and gather statistics. Once the Internet Protocol (IP) address was set the Console program can be remotely accessed from the desktop in order to make changes to the configuration settings.

The second attractive feature is that the access point did not require additional hardware. The Aironet access point is a stand-alone unit and did not need an additional PCMCIA card in order to operate.

There were two drawbacks encountered with the Aironet products. The first is one that, although it was an attractive feature to not require additional hardware, the previous version of the access point (AP-4500) does not support the higher data rates. In order to upgrade to an IEEE 802.11b compliant system the access point would also require replacement. The second disadvantage is that the antennas are mounted to the access point base unit. This requires that the base unit be located in a position where the maximum signal strength is achieved.

B. RECOMMENDATIONS FOR CONTINUED RESEARCH

Even during the course of writing this thesis there were many significant changes taking place in the wireless world. As wireless technology continues to expand, we must remain aggressive in our exploration in order to meet the future needs of the Navy. The results presented in Chapter V are not representative of the performance that would be achieved onboard a ship. This test only presented a comparison of several components presently available. Further evaluation should be conducted in the shipboard environment in order to provide conclusive results of how these components will perform in that atmosphere.

1. Mobile Computer Evaluation

Although not evaluated in this thesis, lightweight portable devices are closely affiliated with the issue of wireless networks onboard naval vessels. Compact mobile devices will afford the user full access to the network whenever and wherever the need arises. Hand held pen type computing devices are becoming more and more apparent in our every day life. They offer the essential flexibility that will be necessary for the navy of tomorrow.

2. Future Evaluation

With the expansion of the wireless market, new products are available almost every day. As discussed in Chapter III, the High Performance Radio Local Area Network (HiperLAN) family of standards appears to be the next area for future evaluation.

On February 4, 2000, the European Telecommunications Standard Institute (ETSI) approved two new guidelines for the HIPERLAN/2 standard which, completes the set of core technical specifications which enables manufacturers to start developing HIPERLAN/2 products. [Ref. 35]

The HiperLAN2 Global Forum, featuring participation from vendors such as Ericsson, Dell, and Nokia, plans to promote the HiperLAN2 standard to enable high-speed connectivity for "next-generation" mobile communications. The first compliant products are expected in the latter half of 2001. Products abiding by the standard will operate in the 5-GHz band, and enable quality-of-service support as well as potential for deploying

multimedia and real-time video applications. Additionally, HiperLAN2 also offers strong security support and presents the possibility of a "plug and play" wireless network. [Ref. 36]

HiperLAN offers the highest data rate of any existing wireless LAN specification. At more than 20 Mbps per channel, and with several channels possible at each location, HiperLAN can support very high data throughput applications, or very high user densities. [Ref. 23]

HiperLAN also performs better than any other standard for typical LAN traffic under conditions of very high load. HiperLAN is very stable, which means that it continues to deliver most of its capacity for traffic even when more traffic is submitted for transmission than it can handle. Some systems collapse under such conditions of overload, and are said to be unstable. This combination of high data rate and high stability make HiperLAN the best high performance system available. [Ref. 23]

The future lies with the development of HiperLAN in the 17 GHz band. In very high bit rate LANs, this development will hopefully enable an increase in data rate transmission of up to 150 Mbps. The continued evaluation of this technology should be conducted to determine which equipment would best suit the needs of the Navy.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. Astolfi, Stephen, "Smart Ship Program." [http://www.dt.navy.mil/smartship/]. 15 September 1998.

2. Debus, Steven M., *Feasibility Analysis for a Submarine Wireless Computer Network Using Commercial off the Shelf Components*, Master's Thesis, Naval Postgraduate School, Monterey, California, September 1998.

3. Rothenhaus, Kurt J., *Distributed Software Applications in Java for Portable Processors Operating on a Wireless LAN*, Master's Thesis, Naval Postgraduate School, Monterey, California, September 1999.

4. Matthews, Mark M., *Analysis of Radio Frequency Components for Shipboard Wireless Networks,* Master's Thesis, Naval Postgraduate School, Monterey, California, December 1999.

5. Lough, Daniel T., Blankenship, T.K., and Krizman, Kevin J., "A Short Tutorial on Wireless LANs and IEEE 802.11." [http://computer.org/students/looking/summer97/ieee802.htm]. July 1997.

6. Yun, X., and others, "Feasibility Analysis of Deploying Wireless Local Area Networks (WLANS) Onboard Submarines and Surface Ships," *Naval Postgraduate School Research*, v. 9, number 3, pp. 1-3, October 1999.

7. WLANA, The Wireless LAN Alliance, "Introduction to Wireless LANs, How WLANs Work." [http://www.wlana.com/intro/introduction/work.html]. 1996.

8. WLANA, The Wireless LAN Alliance, "Introduction to Wireless LANs, Technology Options." [http://www.wlana.com/intro/introduction/wirels.html]. 1996.

9. Institute of Electrical and Electronic Engineers, Communication Standards Information Service, "IEEE 802.11 Wireless Local Area Networks Tutorial." [http://www.comsoc.org.mx/standard/802_11.htm]. 7 June 1999.

10. Institute of Electrical and Electronic Engineers, Inc., *IEEE Standard 802.11-1997*, Institute of Electrical and Electronic Engineers, Inc., New York, NY, 1997.

11. WLANA, The Wireless LAN Alliance, "Introduction to Wireless LANs, Overview: Benefits of WLANs." [http://www.wlana.com/intro/introduction/introbene.html]. 1996.

12. Spread Spectrum Scene, "Introduction to Indoor Radio Propagation." [http://www.sss-mag.com/indoor.html]. 10 December 1998.

13. Sklar, B., "Rayleigh Fading Channels in Mobile Digital Communication Systems Part I: Characterization," *IEEE Communications Magazine*, July 1997.

14. Lucent Technologies, Inc., *WaveLAN Wireless LAN Technology and Market Backgrounder*, Lucent Technologies, Inc., The Netherlands.

15. Zuo, Zhengping, "In-building Wireless LANs." [http://www.cis.ohio-state.edu/~jain/cis788-99/wireless_lans/index.html]. 17 November 1999.

16. Rune, Torben, "HIPERLAN – The Approaching Standard for Wireless LANs." [http://www.netplan.dk/hip.htm]. 14 February 1997.

17. Boer, Jan, "Direct Sequence Spread Spectrum Physical Layer Specification IEEE 802.11." [ftp://stdsbbs.ieee.org/pubs/802_main/802.11/tutorials/tutds3.ppt]. 1996.

18. Champness, Angela, "Understanding the Benefits of IEEE 802.11." [http://www.steinkuehler.de/wavelan_802_11_Benefits.htm]. 24 January 2000.

19. Jain, Raj, "Wireless Data Networking." [http://www.cis.ohio-state.edu/~jain/cis788-97/h_cwir.htm]. 1997.

20. Wirbel, Loring, "Fast-WLAN Scheme Wins IEEE Approval." [http://www.eet.com/news/98/1017news/fast.html]. 17 July 1998.

21. Kesarev, Kiril, "Security Level and Solutions in Wireless and Mobile Data Transfer." [http://www.tcm.hut.fi/Opinnot/Tik_110.300/Tehtavat/mobile_wireless/security_2.html]. 5 September1997.

22. Kiacz, Balazs, "Overview of BRAN Standard." [http://www.etsi.org/bran/branstds.htm]. 3 February 2000.

23. Taylor, Larry, "HIPERLAN Type 1 Technology Overview." [http://www.hiperlan.com/hiper_white.pdf]. June 1999.

24. Ulus, Tolga, "Wireless Local Area Networks." [http://www.mis.boun.edu.tr/ulus/courses/mis221/project/wireless-lans.htm]. December 1998.

25. Essentia Telecomunicazioni, "Why Spread Spectrum." [http://www.essentia.it/spread_spectrum_tutor.htm]. 24 February 2000.

26. Vincent, James, "Spread Spectrum Voice Link." [http://www.sss-mag.com/pastissues/vol3num2/ssvl.html]. 1995.

27. Strategic Microelectronics Consortium, "Spread Spectrum Fundamentals." [http://strategis.ic.gc.ca/SSG/it02072e.html]. 1 March 1996.

28. RadioConnect Corporation, "RadioConnect Spread Spectrum Technology." [http://www.radioconnect.com/tech.html]. June 1999.

29. Andren, Carl, "Modulation Techniques for High Speed WLAN Systems." [http://www.wirelessdesignonline.com/design-features/19980826-2747.html]. 26 August 1998.

30. Kingston Technology Company, "EtheRx Workgroup Ethernet Hubs." [http://www.kingston.com/networking/hubs/kne5tp.asp]. February 2000.

31. Aironet Wireless Communications, Inc., *User's Guide Wireless Access Point for Ethernet and Token Ring*, 1998.

32. Lucent Technologies, *WaveLAN IEEE 802.11 PC Card User's Guide*, 1999.

33. Lucent Technologies, "ORINCO PC Card." [http://www.wavelan.com/products/productdetail.html?id=26]. February 2000.

34. Aironet Wireless Communications, "Freedom to Share." [http://www.aironet.com/default.asp]. February 2000.

35. Kiacz, Balazs, "Core HIPERLAN/2 Standards Approved by ETSI BRAN." [http://www.etsi.org/tbnews/Previous/BRAN_H2_022000.htm]. 11 February 2000.

36. Krill, Paul, "Consortium Makes Wireless Interoperability its Goal." [http://www.cnn.co.jp/TECH/computing/9909/16/hiper.lan.ent.idg]. 16 September 1999.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

No. Copies

1. Defense Technical Information Center 2
   8725 John J. Kingman Rd., STE 0944
   Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, CA 93943-5101

3. Chairman, Code EC 1
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, CA 93943-5121

4. Professor Xiaoping Yun, Code EC/YX 3
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, CA 93943-5121

5. Professor Herschel H. Loomis, Code EC/LM 1
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, CA 93943-5121

6. Mr. Steve Lose 2
   Program Executive Officer, Submarines
   PMS 450T2, NC2 5W64
   2531 Jefferson Davis Highway
   Arlington, VA 22242-5168

7. Mr. Gary Lacombe 2
   171 Branch Hill Rd
   Preston, CT 06365

8. LT Rich McConnell 2
   SRF Yokosuka
   PSC 473 Box 8 No.18
   FPO AP 96349-1400